NPS-SE-06-002

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

OPEN ARCHITECTURE AS AN ENABLER FOR FORCENET

by

Viviane Deering
Tom Hedge
Maria Martinez
Kevin Pugh
Patrick Grates
Sein Kung
Percival Mcarthy
Sasha Radojkovic

September 2006

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA 93943-5001

COL. David A. Smarsh, USAF
Acting President

Leonard A Ferrari
Associate Provost

This report was prepared for the Chairman of the Systems Engineering Department in partial fulfillment of the requirements for the degree of Master of Science in Systems Engineering.

This report was prepared by the Masters of Science in Systems Engineering (MSSE) Cohort Four from the Space and Naval Warfare Systems Center, San Diego:

Authors

Viviane Deering	Maria Martinez	Patrick Grates
Percival Mcarthy	Tom Hedge	Kevin Pugh
Sien Kung	Sasha Radojkovic	

Reviewed by:

David H. Olwell, Ph. D.
Chairman, Department of Systems Engineering

Released by:

Dan C. Boger, Ph. D.
Interim Associate Provost and
Dean of Research

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 2006	Technical report

4. TITLE AND SUBTITLE:
Open Architecture as an Enabler for FORCEnet

5. FUNDING NUMBERS

6. AUTHOR(S) Viviane Deerin, Patrick Grates, Tom Hedge, Sein Kung, Maria Martinez, Percival Mcarthy, Kevin Pugh, Sasha Radojkovic

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this report are those of the author(s) and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE
A

ABSTRACT This project concentrates on implementing network centric military operations with specific threat engagement scenarios using legacy and future warfare systems based on open architecture concepts. These systems may be based at sea, on land or in the air, and provide fire control solutions that match sensed threats to available weapons throughout the battle space. Using a unique methodology, the project provides the following: 1) characterization of the battle space 2) description of the design principles applied and 3) a conceptual design. The conceptual design is then modeled using ARENA® simulation software in an attempt to validate the proposed architecture. The project concentrates on implementing three very specific scenarios: Engage on Remote (EOR), Forward Pass (FP), and Remote Fire (RF). These concepts are applied to the FORCEnet Open Architecture Domain Model using legacy and future Naval systems such as AEGIS Cruisers and Destroyers, DD(x), CG(x), Littoral Combat Ship (LCS), and Joint Land Attack Cruise Missile Defense Elevated Netted Sensor System (JLENS). As a part of the above scenarios, the presentation will address specifics on best shooter selection. The resulting functional architecture and data flows transform concepts into real engagement methods. These methods will match the Detect-Control-Engage (DCE) sequence with Observe-Orient-Decide and Act (OODA), and employ current methods of data fusion from various platforms to provide a true integrated fire control solution. Combat identified threats on the network can then be matched to any available weapons on the network, and the preferred shooter selected can efficiently engage the threat. Thus, the effective and efficient use of all sensors and weapons available in the battle space becomes possible.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Open architecture concepts; data flows; network centric military operations; Engage on Remote (EOR), Forward Pass (FP), and Remote Fire (RF).	145
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

THIS PAGE INTENTIONALLY LEFT BLANK

OPEN ARCHITECTURE AS AN ENABLER FOR FORCENET

ABSTRACT

This paper discusses an approach to implementing a FORCEnet architecture based on open architecture concepts. Using an architecture-focused methodology, the approach provides the following:

1) Characterization of the battle space
2) Description of the design principles applied and
3) Conceptual design.

The conceptual design is then modeled using ARENA® simulation software to validate the proposed architecture.

The paper concentrates on implementing three very specific scenarios: Engage on Remote (EOR), Forward Pass (FP), and Remote Fire (RF). The Open Architecture Domain Model is applied to the functional model of these scenarios to develop the architectural concept. As a part of the above scenarios, the paper addresses specifics on best shooter selection. The resulting functional architecture and data flows transform concepts into real engagement methods. These methods match the Detect-Control-Engage (DCE) sequence with Observe-Orient-Decide and Act (OODA) paradigm using current data fusion concepts to provide an Integrated Fire Control (IFC) solution. Identified threats on the network can then be matched to any available weapons on the network, and the preferred shooter selected can efficiently engage the threat. Thus, the effective and efficient use of all sensors and weapons available in the battle space becomes possible.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS

ACRONYM	DEFINITION
AMA	Automated Management Aids
A-RCI	Acoustic Raid COTS Insertion
ASCM	Anti-ship Cruise Missiles
AOR	Area of Responsibility
ASD(NII)	Assistant Secretary of Defense, Network and Information Integration
BLII	Base Level Information Infrastructure
BMMP	Business Management Modernisation Program
C2	Command and Control
CEC	Cooperative Engagement Capability
CEP	Cooperative Engagement Processor
CID	Combat Identification
CINC	Commander-In-Chief
CNE	Computer Network Exploitation
COA	Course of Action
COP	Common Operational Picture
COTS	Commercial Off-The-Shelf
CR #	Change Request Number
CSG	Carrier Strike Group
CTN	Core Transmission Network
CTP	Common Tactical Picture
DCE	Detect, Control, Engage
DCN	Document Control Number
DIA	Defense Intelligence Agency
DIAP	Defense Information Assurance Program
DISR	Defense Information Technology Standards Registry
DMI	Data Management and Interoperability
DoD	Department of Defense
DRM	Distributed Resource Management
EDM	Engineering Development Model
EHF	Extremely High Frequency
EoR	Engage On Remote
ESG	Expeditionary Strike Group
EW	Electronic Warfare
FAA	Functional Area Analysis
FAM	Functional Area Manager
FCP	Fire Control Picture
FCS	Fire Control Solution
FCQ	Fire Control Quality
FFBD	Functional Flow Block Diagram
Fn/OA	FORCEnet Open Architecture
FP	Forward Pass
FOS	Family of Systems
FRU	Firing Unit

ACRONYM	DEFINITION
FTA	From The Air
FTL	From The Land
FTS	From The Sea
FY	Fiscal Year
GES	Global Information Grid Enterprise Services
GIG	Global Information Grid
GCCS-M	Global Command and Control System Maritime
HF	High Frequency
IABM	Integrated Architecture Behavior Model
IDEF	Integrated Definition for Function
IEE	Information Exchange Effectiveness
IER	Information Exchange Requirement
IFF	Identification Friend or Foe
IFC	Integrated Fire Control
IP	Internet Protocol
IS	Information Superiority
ISNS	Integrated Shipboard Network System
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology
IWS	Integrated Warfare Systems
JDL	Joint Directors Laboratory
JLENS	Joint Land Attack Cruise Missile Defense Elevated Netted Sensor System
JSSEO	Joint SIAP System Engineering Organization
LAN	Local Area Network
LCS	Littoral Combat Ship
LoR	Launch on Remote
MK2	Mark 2
MOD3B	Module 3 B
MCP	Mission Capability Packages
MIDS	Multifunction Information Distribution System
NAVSEA	Naval Sea Systems Command
NCES	Net-Centric Enterprise Services
NCW	Network-Centric Warfare
NIFC-CA	Naval Integrated Fire Control-Counter Air
NSWC	Naval Surface Warfare Center
NR	Net Ready
OA	Operational Architecture
OACE	Open Architecture Computing Environment
OODA	Observe, Orient, Decide and Act
OV	Operational View
P2P	Peer-to-Peer
PCP	Peer Computing Program
PEO	Program Executive Office
RF	Radio Frequency
RL	Remote Launch
ROI	Return On Investment
RU	Remote Unit
RWO	Real-World Objects

ACRONYM	DEFINITION
SA	Situational Awareness
SSDS	Ship Self Defense System
SHF	Super High Frequency
SIAP	Single Integrated Air Picture
SOS	Systems of Systems
SP	Situation Prediction
SRM	Sensor Resource Management
TBD	To Be Determined
UHF	Ultra High Frequency
U.S.	United States
WAN	Wide Area Network

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

This paper discusses an approach to implementing a FORCEnet architecture based on open architecture concepts. Using architecture-focused methodology, the approach provides the following:

1) Characterization of the battle space

2) Description of the design principles applied and

3) Conceptual design.

The conceptual design is then modeled using ARENA® simulation software to validate the proposed architecture.

The primary focus is on implementing three very specific scenarios: Engage on Remote (EOR), Forward Pass (FP), and Remote Fire (RF). The Naval Sea Systems Command Program Executive Office (PEO) Integrated Warfare Systems (IWS) Open Architecture (OA) domain model is applied to the functional model of these scenarios to develop the architectural concept. The IWS OA domain model is decomposed to the basic functions employed in specifically implementing these three scenarios. The resulting functional architecture and data flows transform concepts into real engagement methods. These methods match traditional algorithms such as Detect-Control-Engage (DCE) and Observe-Orient-Decide and Act (OODA) using current data fusion concepts to provide an Integrated Fire Control (IFC) solution. The system is then recomposed to the OA domain model level, and compared to the original conceptual IWS OA domain model yielding similarities and differences based on actual implementation. Proposed changes and improvements to the model are then suggested based on the analysis. A brief summary of the results follows:

1. The **Search and Detect** functional will assign an immediate low level identification of a track so that it can be added to the network almost immediately for correlation to tracks on other platforms. Higher fidelity

combat identification of tracks can then be performed later in the process as originally conceptualized in the IWS OA domain model.

2. **Weapon Assets and Services** block was completely eliminated primarily based on its functions being moved to other functional areas with improved efficiency.

3. **Force Planning and Coordination** block was also eliminated. Joint Battle Force Orders (JBFO) and Battle Group Orders (BGO) will be broadcast to all platforms simultaneously. The orders will be processed through common services and received via EXCOMM.

4. **EXCOMM** block is considerably expanded, and will assume the "event status" of the old weapon/asset services and integrate more directly with common services. EXCOMM will call on various communication paths dependent on data priority and security requirements for FCS transmission, track/threat updates, and direct receipt of intelligence data.

With these improvements, identified threats on the network can then be matched to any available weapons on the network, and the preferred shooter selected can efficiently engage the threat. Thus, the effective and efficient use of all sensors and weapons available in the battle space becomes possible.

In conclusion, the analysis performed for this research project has exposed potential functional boundary limitations in the currently proposed PEO IWS OA domain model as presented, and a revised OA Functional Domain model has been offered for consideration. Through simulation development, test execution and the use of systems engineering techniques, this re-structured model has been evaluated and appears to satisfy OA and FORCEnet requirements.

Additional benefits may be gained from expanding the simulation model to increase the number of FORCEnet platform participants so as to determine the point at

which the OA model becomes inefficient and/or ineffective. OA specifications and system boundary descriptions will eventually attain capacity levels with respect to data flow. This point of diminishing returns relative to battle space size should be identified, realized, and modeled.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

FORCEnet refers to the architectural and operational framework behind the network centric warfare concepts of the Navy's vision for the 21st century, Sea Power 21 (Clark, 2002). In a letter from the Deputy Chief of Naval Operations CNO (Warfare Requirements and Programs) dated 6 JAN 2006, the implementation of Open Architecture (OA) principles across the Navy Enterprise was set forth as a requirement. For FORCEnet to be effective, the nodes that comprise the network must employ standardized joint protocols, common algorithms and data packaging, and interoperate in a seamless and efficient manner. The architecture of today's war-fighting computer systems cannot support the missions of the emergent Sea Power 21 without embracing and becoming OA compliant. Gathering and exchanging information effectively is critical to the network centric warfare capability. Sensor derived data from the networked platforms are processed, identified, exchanged, then correlated using common data fusion techniques. Resultant Fire Control solutions are generated which match the optimal platform to the optimal weapon to the highest priority threat. These solutions encompass all weapons from all platforms to provide an effective coordinated warfare effort, essentially selecting and designating the "best shooter" to engage, intercept, and hopefully destroy the threat.

Successful implementation of the FORCEnet strategy will undoubtedly require a dedicated core of warfighters and systems engineers to design and execute a seamless operation of what is called a System of Systems (SOS) or Family of Systems (FOS). As stated in Sea Power 21, this effort must be administered From the Sea (FTS), From the Land (FTL), and From the Air (FTA). This project will concentrate on FTS, and will address three specific engagement scenarios representative and typical of a FORCEnet tactical environment: Remote Launch (RL), Forward Pass (FP), and Engage on Remote (EOR). These scenarios have been described in detail in supporting reference documents used as a basis for this thesis (Young, 2004). The goal of this project is to reconstruct and validate one of the currently proposed FORCEnet Open Architecture (OA)

functional schemes, through a top-down, then bottom-up progression, and suggest possible model alternatives and improvements.

B. MOTIVATION

FORCEnet is defined as the operational construct and architectural framework for naval warfare in the Information Age, integrating warriors, sensors, command and control, platforms and weapons into a networked, distributed combat force. Narrowing this broad view to the concept of FTS and Naval Air defense, an evaluation of FORCEnet functional concepts may be accomplished through an examination of the following two capability-driven warfighting requirements or Mission Capability Packages (MCPs):

1. **Time Critical Targeting**: Time Critical Targeting refers to the ability to detect, track, engage and assess time sensitive targets. Time sensitive targets are those threats that have an extremely limited window of vulnerability or opportunity where they can be detected before becoming hidden. Medium-range missiles such as Theatre Ballistic Missiles (TBM) fall within this category. Essentially this corresponds to the warfighter's ability to perform an optimal, seamless, execution of the kill chain.

2. **Cruise Missile Defense** (NRC, 2005): An effective Cruise Missile defense capability relies on full joint integration of all available defense assets and the implementation of a family of systems at the joint level to accomplish the mission.

FORCEnet concepts and implementation methods are currently being developed across many Department of Defense (DoD) activities. However, detailed FORCEnet implementation requirements and specifics regarding how open architecture operates within the FORCEnet construct have not been fully developed. Within the constraints of the FORCEnet Naval Air defense mission, integrated fire control systems design, and concepts of operation have not been completely defined and analyzed beyond providing high-level domain models. This project attempts to address this gap through the use of FORCEnet and open architecture principles to allocate partitioned system functionality from the perspective of air defense engagements conducted within an integrated fire control systems model. The air defense operational concepts are translated into notional system process flows, and from this, a supporting functional design architecture model is developed.

This systems engineering analysis effort will attempt to develop a conceptual match between operational and system architecture requirements using the technical requirements of the Open Architecture Domain Model. The analysis will be performed using the previously stated Integrated Fire Control (IFC) scenarios of Remote Launch (RL), Forward Pass (FP), and Engage On Remote (EOR). Also addressed will be the concept of "Best Shooter." The analysis will elaborate on these basic mission capabilities and apply them to battle space defensive measures.

The concept of managing warfare resources across the battle space (e.g. sensors, weapons, communication devices) in concert with using data fusion techniques and automated decision-making aids is attempted based on the these three operational concepts and modeled using a simulation program application called ARENA®. The resultant output provides insight into currently proposed architectural models and possible alternative methods.

C. PROBLEM STATEMENT

The tasking for this research project, as stipulated within the **Open Architecture as an Enabler FORCEnet** Statement of Work (SOW, Appendix G), is being performed in support of a continuing series of FORCEnet research efforts being performed by Naval Postgraduate School Masters of Science in Systems Engineering (MSSE) students. This task is unique in that it investigates the role of FORCEnet within the Open Architecture (OA) Functional Domain Model whereas the other tasks investigate the concept of coalition Fn and its related performance and acquisition issues. The integration of OA within FORCEnet is inevitable, but the detailed implementation requirements regarding how open architecture operates within the FORCEnet construct have not been fully defined or developed.

The intent of this project is to examine the recently proposed PEO IWS OA Domain Model through various functional levels of decomposition, to determine if there is a conceptual match between FORCEnet operational and OA system architecture requirements. The analysis will use the Integrated Fire Control (IFC) elements of the previously stated MCPs, to construct Remote Launch (RL), Forward Pass (FP), and Engage on Remote (EOR) scenarios. The concept of management of warfare resources

across the battle space, such as sensors, weapons, and communication devices, in concert with new methods of data fusion techniques and automated decision making aids is attempted based on the three operational concepts and modeled using the ARENA simulation program. The resultant output provides insight into improved architectural models and alternative methods.

D. OBJECTIVES

The analysis intends to accomplish the following primary objectives:

1. **Characterization of the problem space**: the identification of current system deficiencies as well as existing constraints inherent in the operational environment for the purpose of characterizing, understanding and bounding the problem space. The analysis will translate relevant operational imperatives into system engineering structures (concepts, functions, requirements, solutions) necessary to fully develop the FORCEnet OA (Fn/OA) concepts.

2. **Design principles**: the formulation of principles for the design and architecting of OA and IFC capabilities. The design principles will serve as guidelines for the development of system solutions. Design principles will consider known limitations and constraints of the operational environment such as communication challenges (unreliability, ad hoc mobile networks, limited bandwidth, etc.) and operator interactions (command authority, manual overrides, etc.).

3. **Conceptual design**: method development, architecture, and a conceptual framework that addresses the problem space and is based on design principles for a distributed system of automated decision aids for optimally managing warfare resources operating within a collaborative environment

4. **Functional representation and decomposition**: the representation of system concepts through functional description and decomposition as well as system architecting and simulation. Develop representations, models, and methods to express automated resource collaboration concepts and solutions in the context of the Fn/OA architecture domain.

5. **Analysis of key capabilities**: the identification and evaluation of technologies and research areas key to the FORCEnet OA concept. Technology areas that will be researched and analyzed include:

a. Data fusion techniques and algorithms
b. Resource management scheduling and optimization methods
c. Weapon and sensor management for aerospace warfare
d. Automated management aids
e. Engagement functionality, initialization, and control

f. Situation prediction
g. Tactical planning and battle management

E. METHODOLOGY

The architectural view of the PEO IWS model provided the basis and starting point for this project. From the systems engineering perspective, questions such as the following needed to be asked: Is this design feasible? Will it satisfy FORCEnet IFC functional, system, and operational requirements while maintaining and complying with OA design principles? Will a simulation modeling and test process identify any deficiencies and lead to recommendations for improvement? To evaluate and answer these questions, a unique architectural-based systems engineering methodology was formulated and used.

The PEO IWS OA model provided the initial architectural framework and conceptual representation of expected FORCEnet domain rules, resources and functional relationships. To validate this model, the functional and modular integration needed to be proven to determine if it would support likely FORCEnet the IFC elements of the Mission Capability Packages. To better understand the modular interaction, descriptions of the functional blocks were developed and further modular de-composition was performed. This was then repeated until three levels of functional de-composition had been achieved. Data inputs and outputs, communication flows and control points were added based on three typical Integrated Fire Control scenarios. This level of functional characterization provided the path necessary to move forward with the simulation modeling and development. With simulation development and test trial runs, feedback was provided as to whether data flows, modular and node interactions were valid and

optimal. Iterations to the simulation and functional models were then performed to better functionally represent the interplay involved. The functional model was refined and compared to the PEO IWS model to complete the process.

II. LITERATURE

The literature review section has been divided into three subsections. The first section presents an overview of the literature used to define the scope of the problem space used as a basis for this project. The second section reviews some of the more pertinent and informative research material available on FORCEnet OA implementation to date and identifies positions that should be considered when developing a detailed, scenario based architecture. Some of the works reviewed provide a basis to forecast the manner in which FORCEnet OA will be implemented. Several of these forecasts are compared with the results and conclusions derived from this project. The third section reviews several of the early and more recent notable expert opinions on proposed FORCEnet OA implementation strategies.

A. DEFINING THE PROBLEM SPACE

An OA system has been defined as a non-proprietary, commercially available computer system that supports the following attributes with minimal cost and minimal impact on existing system components:

- Use of public, consensus-based standards
- Adoption of standard interfaces and protocols to facilitate new or additional systems capabilities for diverse applications
- Adoption of standard services and defined functions
- Use of product types supported by multiple vendors
- Selection of stable vendors with broad customer base and large market share
- Interoperability with minimal integration requirements
- Ease of scalability and upgradeability
- Portability of applications

But what exactly does it take to achieve an OA implementation in a FORCEnet construct? There are several key ingredients necessary:

1. Well-defined and easily understandable system boundaries at various levels must be constructed.

2. The interfaces that exist at these system boundaries must be described in detail using established commercial or Department of Defense (DoD) standards.
3. Starting at the highest level of system and boundary descriptions, subsystem descriptions and interface definitions must be capable of two or more layers of decomposition based on established and traditional system engineering practices.

In the "FORCEnet Implementation Strategy" guide (NRC 2006), functional boundary principles are outlined that are partitioned yet collaborative (Figure 1).

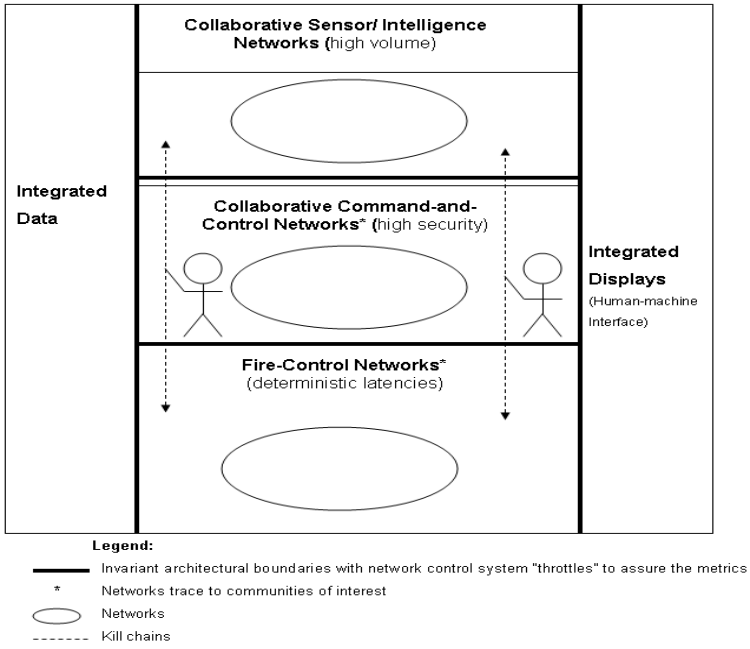

Figure 1. Boundaries Between Functions in FORCEnet Information Architecture (FORCEnet Implementation Strategy, National Research Council, 2006)

Using the principle behind this conceptual model, the Naval Sea Systems Command (NAVSEA) Program Executive Office, Integrated Warfare Systems (PEO IWS) division has developed an OA Domain Model consisting of a first level functional decomposition. The PEO IWS OA Domain Model (Figure 2) illustrates how the various key functions necessary within the FORCEnet construct may be allocated and identifies

the expected data flow interactions between the various sub-functions. With the PEO IWS OA Domain Model Concept used as the starting point, this research project will proceed to use one of the well recognized Systems Analysis Tools, the Functional Flow Block Diagram (FFBD), as defined in *Systems Engineering and Analysis* (Blanchard and Fabrycky 1998) to decompose each functional block down two additional levels and construct a simulation model to support these processes. The simulation model is then used to test and apply specific FORCEnet mission scenarios and validate the PEO IWS OA Domain Model Concept using a bottom up systems engineering approach.

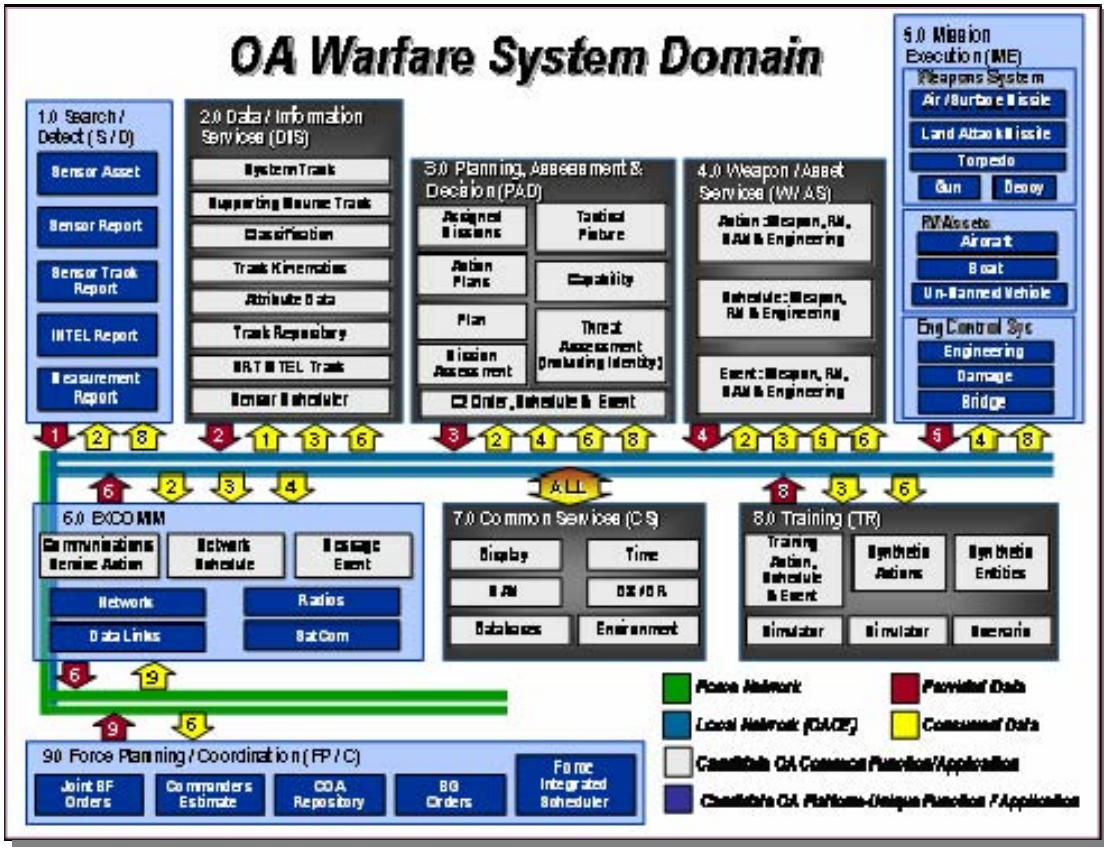

Figure 2. PEO IWS OA Domain Model Concept (Combat Identification for Naval Systems in an Open Architecture, Strei, 2003)

As described in the 2006 publication "FORCEnet Implementation Strategy" by the National Research Council (NRC), boundary definitions and the granularity with

which they are defined are keys to the successful OA implementation within the FORCEnet arena. The total number of boundaries must not exceed those that can be reasonably managed, and the cost to maintain those boundaries must not exceed the benefits achieved through interoperability.

Although this project focuses on boundaries more than standards, the following six categories of core architectural elements have been considered:

1. Intelligence, surveillance, and reconnaissance
2. Weapon systems
3. Command and control support
4. Network services
5. Networks
6. Communication Systems

Using these architectural elements and well established commercial and DoD standards to define the "Open" in OA, virtually any sensor can be accessed by any command and control system that can direct any fire control system using any weapon. Human monitoring of the network will be required, however, and human intervention and overrides are considered inherent in the design.

The ultimate success of FORCEnet relies heavily on having a time critical network. Battle space size and the ability of the Battle Force to effectively manage and dominate this space are directly related to the speed of data collection and transmission and its efficient, secure, dissemination across the network. This project assumes a decentralized decision-making concept. This means that the decision-making process supporting the FORCEnet mission is not constrained to any one platform. Based on sophisticated data fusion techniques, high priority data is throttled across system boundaries so that local and remote decision-making can quickly respond to high priority threats and effective "best shooter" decisions can be made. In some cases however, the "best shooter" may not be capable of detecting the threat with their local sensors, and only an awareness of the threat will emanate from the network. The quality of network

service must be sufficiently high enough so that commanding officers on both the firing and controlling platforms are fully confident in the validity of the threat and the ability to execute the engagement. Metrics must be established that monitor track detection time, identification time, and decision time. Performance metrics will drive change management not only of the interface standards, but of the system development spirals. Reliable, timely, and accurate data is critical to the success of the system.

Vulnerabilities of FORCEnet must also be considered when selecting interface standards and establishing system boundaries for the OA design. Many of these vulnerabilities are similar to those encountered during daily use of the Internet. Although unauthorized entry, sabotage, poisoned data, and denial-of-service are a few of the difficult challenges that should be factored into FORCEnet OA implementation, they are not within the scope of this project. Vulnerability as a result of system complexity and the need for graceful degradation when system components fail however, were considered during project development

Several key principles outlined in "FORCEnet Implementation Strategy" (NRC 2006), were considered during project and concept development:

- Partitioning common functions in a common consistent manner
- Minimizing the number of interfaces involved
- Cost and maintenance associated with network management
- Measuring and prioritizing data flows
- Applying system concepts to specific missions to validate results.

B. IMPLEMENTING FORCENET – WORK ACCOMPLISHED TO DATE

1. Legacy Models: When considering Unit-level and Force-level network centric battle operations, an examination of the legacy conceptual models upon which the PEO IWS OA Domain model is based, is worthwhile. The three most common models are:

a. Detect, Control, Engage (DCE) sequence

b. Observe, Orient, Decide and Act (OODA) sequence

c. Data Fusion Model.

The DCE model is one of the earliest models and a common tool that has been used for many years. The OODA loop and Data Fusion model, developed by Colonel John Boyd and the Joint Directors Laboratory (JDL) Data Fusion Group, respectively, were both introduced in 1987. In a paper titled "A Self-Consistent Context for Unit and Force Level Tactical Decision-Making", Luessen provides a good illustration on how these three models may be logically combined (Figure 3).

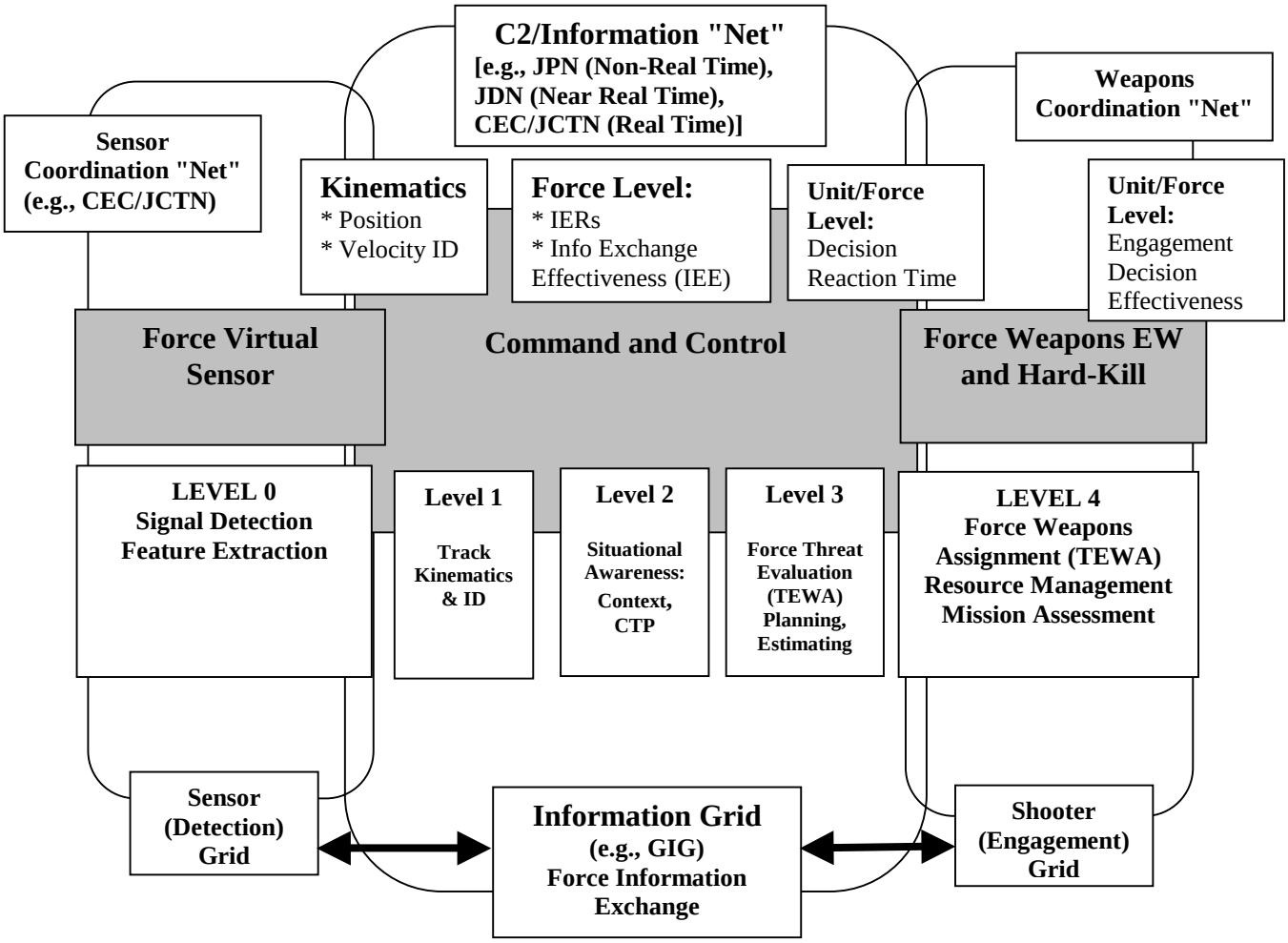

Figure 3. Integration of DCE, OODA and Data Fusion Models (A Self-Consistent Context for Unit and Force Level Tactical Decision-Making, Luessen, 2003)

Although not within the scope of this paper, each portion of the PEO IWS OA Domain Model could likely be mapped to a portion of the DCE, OODA, and Data Fusion Integration model. Additionally mirroring the OA Domain model, a lower level functional decomposition of this model could also be performed.

The integrated diagram (Figure 3) depicted by Luessen illustrates the manner in which Information Exchange Requirements (IERs) and Information Exchange Effectiveness (IEE) are directly related to the transmission of information across the Battle Force and the interoperability effectiveness within Battle Force. Luessen begins with the DCE sequence at the Combat System Unit level, expands this sequence to the Force level, then applies the fusion processes at the Battle Force level to complete the Force-Level Command and Control (C2) representation of the engagement decision-making process. The accuracy of the data and the efficiency of its transmission from signal detection at the sensor grid level (Level 0) through the Common Tactical Picture (Level 2), then through the Force-level weapon assignment and coordination level (Level 4), are the keys to effecting successful execution of the Battle Force engagement sequence. Both Unit and Force-level reaction time and the quality of the engagement decision, directly speak to the ability of the Force-level players to execute the mission and dominate the battle space. In this environment, C2 Operators are able to exploit both the common operational and tactical pictures to process and manage a clear coherent, unambiguous (non-dual) tracking picture where tracks of high interest and threats can be readily identified and prioritized. This heightened situational awareness enables three key capabilities:

a) The ability to effectively prosecute and engage threats
b) The ability to maintain positive identification of non-threats
c) The ability to minimize wasted resources in both the sensor and weapon grids

This diagram also illustrates that provided a minimum of three pieces of data are available, one decision-making process can be effectively employed at both the Unit and Force levels. These data points are:

a) track kinematics

b) track identification

c) the engagement status of the track

Since 1987, the same general data fusion model has been used and deployed at the platform and command and control level. In a paper titled "Revisions to the JDL Data Fusion Model" (Steinberg et al, 1999), Steinberg provides us with a good pictorial representation of the data fusion process (Figure 4).

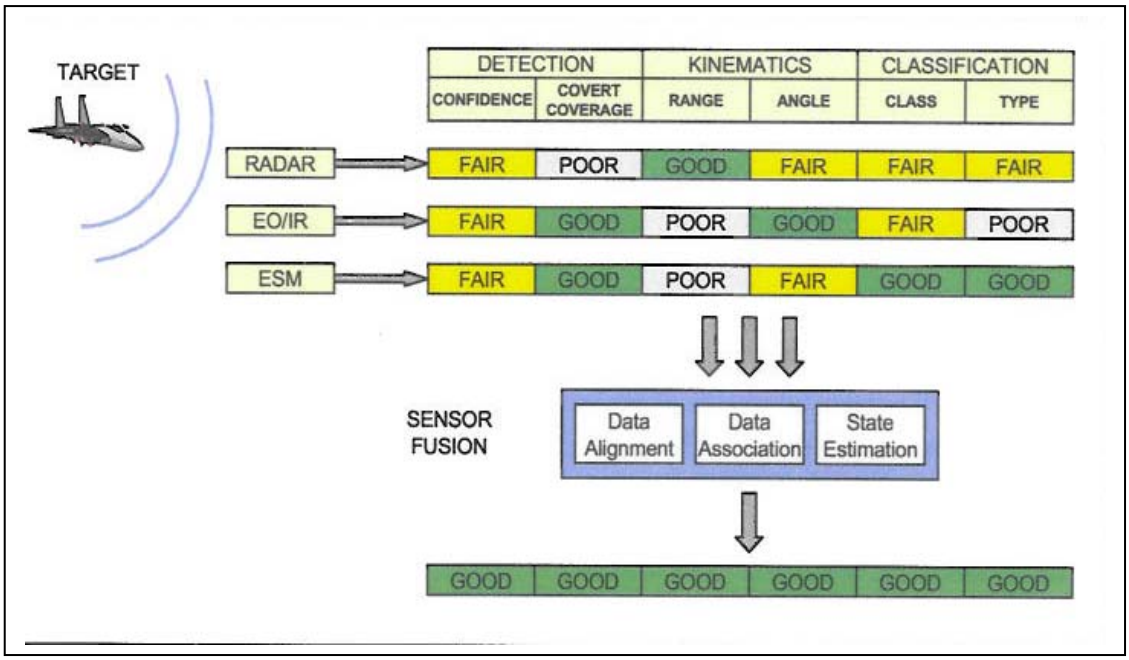

Figure 4. Data Association uses overlapping sensor capabilities so that State Estimation can exploit their complimentary capability (Revisions to the JDL Data Fusion Model, Steinberg, 1999)

Employing the Data Fusion Levels 0 through 4 functions first identified by Luessen (Figure 3), automated algorithms process the information generated in Figure 4, reducing it down to a quality fused output that operators can use with confidence to make decisions and take the best course of action. As Steinberg, Bowman, and White point out, however, there is more that is required within the data fusion loop. Because data fusion is used to estimate the state of some aspect of the real world, the process must also consider

what data is available to the intended target, and how the intended target may perceive that data and react. The data that is available to the target is termed the *informational state* and how the target estimates the world state is called the *perceptual state.* Using this means of data association, data fusion can make a hypothesis about the target and plan possible responses. Figure 5 illustrates how the data that is available to each entity in the relationship may be perceived, and how they may be related back to the physical state for making a more informed and substantiated decision. In developing the proposed architecture for this project, consideration was given to the JDL and other data fusion techniques.

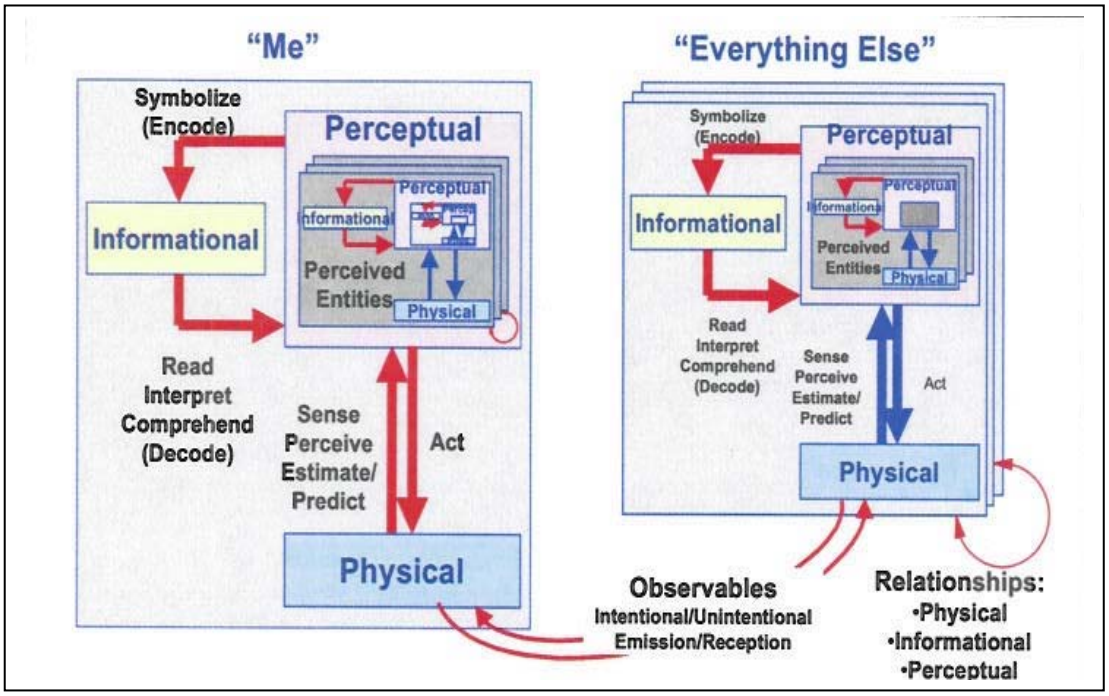

Figure 5. Information available to each entity, perceptions, and relation back to the physical (Revisions to the JDL Data Fusion Model, Steinberg, 1999)

2. Integrated Fire Control: Advances in Network Centric Warfare (NCW) technology, and its implementation, enabled the development of advanced fire control systems and allowed disbursed friendly forces, operating in a common tactical environment, to act seamlessly together as a virtual single unit to detect, engage, and destroy aerospace targets. Fundamental to this ability is the development and

employment of NCW capability within the Navy and Joint Forces. As stated in "Integrated Fire Control (IFC) for Future Aerospace Warfare" (Young, 2004), “Future advances in fire control for aerospace warfare depend largely on a Network Centric Warfare (NCW) foundation that enables the collaborative use of distributed warfare assets for time-critical aerospace operations.”

IFC is defined as the ability of a weapon system to develop fire control solutions from information provided by one or more non-organic sensor sources; conduct engagements based on these fire control solutions; and either provide mid-course guidance (in-flight target updates) to the interceptors based on this externally provided information or in certain cases, have them provided by a warfare unit other than the launching unit. As stated in the "SIAP Operational Concept" (Young, 2002), in order for IFC to be effective, warfare platforms must have the ability to share engaged target information in real-time and eliminate correlation errors as though the information was produced by a single unit using its’ own organic sensors.

From an operational perspective, IFC collaborative efforts take several forms and each requires various levels of coordination and data sharing. In her paper, Young introduces six types of operational perspectives or variants of IFC.

a. Precision Cue: a remote unit cues a local unit to detect and engage target with local sensors and weapons.
b. Launch on Remote (LOR): remote data is used to initiate a local missile launch without holding the target locally; local data is used to support mid-course and terminal missile guidance phases.
c. Engage on Remote (EOR): remote data is used to support all engagement phases of a locally launched missile.
d. Forward Pass (FP): control of an in-flight missile is handed off to another unit to complete the engagement.
e. Remote Fire (RF): a launch decision to fire a local missile is made by a remote unit; either the local or remote unit can control the engagement.
f. Preferred Shooter: when the optimum weapon, or weapons, from a group of collaborative warfare units is selected to intercept a target threat.

Although the six variants above can be thought of as requiring separate processing paths within a system to complete, in a truly integrated collaborative fire control system, each scenario would use common processing architectures both at the local level and at the collaborative systems level. Collaboration between weapons units to achieve true IFC requires that systems be designed from a force-centric perspective where all resources for the weapons engagement are considered a system of systems using common algorithms and common processing. Young states some of the design challenges needed to achieve IFC,

> (an) . . . IFC challenge lies in the necessary paradigm shift ofengagement functionality moving out of weapons systems and instead being performed by common processors across warfare units.

In a non-IFC environment, each warfare unit and their respective weapon systems are focused on their own ability to engage and whether it can intercept the target within its own engagement area. The weapon system does not have a broader, force centric perspective to draw from and cannot determine if it is the best shooter in the Force, as it will only consider local sensor support.

When considering an IFC system design, many concepts must be well thought out prior to implementation. This includes the use of centralized or decentralized communications and control architectures, levels of automation, and control authority of weapons assets across multiple units. Most of these concepts are beyond the scope of this project, but ideally (as proposed by Young) the IFC concept will be based on the following three fundamental systems characteristics:

1. dynamically updateable doctrine
2. decentralized architecture and synchronized information,
3. doctrine and decision aides.

Furthermore, Young has identified four key capability requirements to enable the IFC concept:

1. Shared Situational Awareness (also described by Leussen)
2. Determining the Best Course of Action (COA)

3. Distributed Resource Management (DRM)
4. Embedded IFC Planning

Shared Situational Awareness (SA): SA is the ability of distributed units to gain a common understanding of the tactical situation, to include the threat, defended assets, available resources, and the constraints in which the systems must operate. This important capability relies on each warfare unit using common data processing and data fusion algorithms to develop a tactical picture that accurately represents the ground truth target data and current operating environment. Shared situational awareness relies on appropriate information architecture to enable the sharing of data between units. For the purpose of this project, this architecture is assumed to be the implementation of FORCEnet among all participating units. The architecture must remain flexible and maintain the ability to share the different time domains of tactical data. Time domains of data range from non-real time information on distant targets, or potential launch platforms from intelligence sources, to virtual real-time update rate exchanges required to calculate accurate fire control solutions on high-speed maneuverable targets such as anti-ship cruise missiles (ASCM).

Determining the Best Course of Action (COA): The ability to determine the Best Course of Action involves predicting the various operational situations and hypothesizing about the effects of alternative COAs. Predicting enemy COAs allows for effective resource management of collaborative surveillance, tracking, and weapons assets based on the confidence levels associated with enemy capabilities and intentions. This is primarily accomplished through automated war-gaming methods that are beyond the scope of this project.

Distributed Resource Management: DRM is used to enable and optimize the use of distributed weapon assets used in an IFC environment. It is the capability that allocates the prioritized tasks to the optimum sensor and weapons resources. Task prioritization must be updated automatically and continually for optimization of assets and to determine “best shooter” scenarios. It must take into account both system failures and new resources joining the Force to provide for allocation of available resources at all

times during critical windows of the engagement. DRM, with particular emphasis on sensor management, will be addressed in greater depth when NCW based command and control is discussed.

Embedded IFC planning: Embedded IFC planning allows planners to establish engagement doctrine to guide automated IFC systems in decision-making capabilities. These doctrines can be preloaded into the system based on information regarding the anticipated operating environment and can also be modified dynamically using collaborative means so that all systems are operating from the same set of rules and decision-making guidelines.

3. Combat Identification (CID): The basic construct in establishing a unified Force-Level battle space where well-coordinated combat decisions can be effected is the presence of a unified CID process. In the "Combat Identification (CID)" white paper generated for PEO IWS (Young 2006), Young explores the current state and scope of CID capabilities and examines what levels of development and maturation are necessary to support Joint Single Integrated Air Picture (SIAP) and the Navy's future immersion in OA.

The objective of an effective CID process involves the accurate, timely and sustainable characterization and classification of tracks to facilitate early threat and resource awareness and enable optimal weapon engagement planning and execution in a distributed shared environment. Invariably, any improvements in this area further enhance confidence in situational awareness and optimize command and control level decision-making.

The current means to ascertain and identify battle space objects has been through a combination of the following:

a. Identification Friend or Foe (IFF)
b. Local sensor data
c. Intelligence, Surveillance, and Reconnaissance (ISR)

Two future capabilities proposed by Young are the use of a centralized geographical database and the implementation of a shared resource picture. The geographical database concept would maintain and monitor the friendly forces picture

within a given region. The location, size, status and identity of all Joint and Coalition Forces would be provided, automatically updated as locations change, and periodically synchronized to allow all units a common friendly forces tactical picture. The resource picture is essentially a complement to the "friendly force" picture, but depicts data from friendly force resources such as sensors, weapons, communication links, etc. This data provides the information necessary to perform collaborative resource management across the Battle Force. Young reiterates that CID systems of the future will undoubtedly need to adopt all five of these methods, combining the information from Intelligence Sensors (Intel) and IFF with remote and local fire-control and surveillance radars through data fusion and process refinement. Figure 6 illustrates Young's concept of a CID fusion engine and the input and output relationships involved.

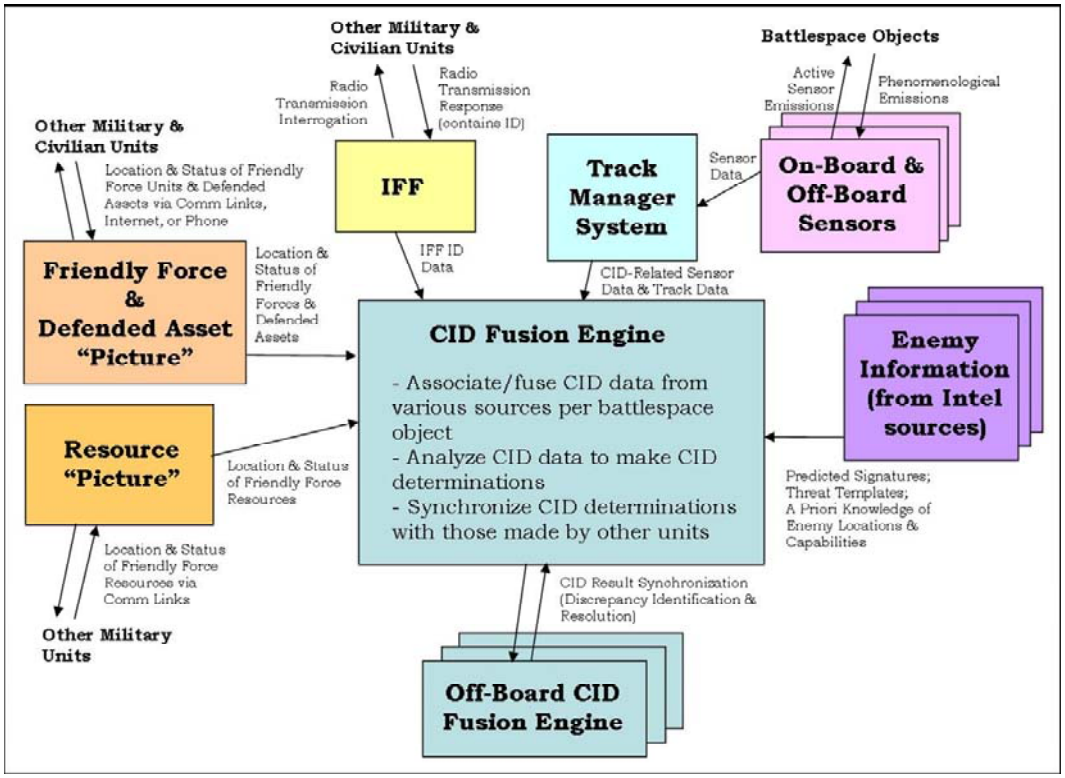

Figure 6. Future CID Capability (Combat Identification, Young, 2006)

According to Young, future CID systems should have the following characteristic capabilities, all of which are inherent to the Open Architecture paradigm:

a. **Common CID deterministic results**: Each units CID process will implement the same logic path, rule sets, algorithms, and prioritization schemes, thus ensuring cohesion within the common operational environment and rule out ambiguity and uncertainty in the assessment process. CID systems will qualify information sources and assign the resultant objects (tracks) confidence levels based on the quality of the data source. This duplication scheme will ensure a high level of shared situational awareness and a distribution of common results among the units. The commonality of these results will subsequently minimize the variability in command and control decision-making within the FORCEnet and could greatly reduce if not eliminate fratricide. Common CID Capability will rely on a networked communication system among the FORCEnet units that can relay CID related information in a time-critical fashion.

b. **Common CID Functionality**: As previously stated, units will need to obtain, share, process, perform object identification and resolve differences in accordance with the "capabilities of the sensor and communication capabilities as well as the ability to automate and use other data/information sources such as Intel, friendly force, defended asset, and resource status information". Functions need to consider questions such as:

- **"**Does the system use all available data?"
- **"**Does the system properly evaluate the "goodness" of the data and calculate confidence levels which accurately reflect this?"
- "Are multiple CID systems able to make identical CID determinations?"

c. **Support Joint Warfare Operating Environment**: Integration of Naval, Marine, Army, Air Force and coalition forces is one of the key

principles to ensure FORCEnet fully exploits the management, range and utilization of available weapons and resources. The more encompassing and open FORCEnet is with respect to the current and emergent Joint services, the greater the improvement in situational awareness. Common CID practices designed using OA principles will facilitate implementation across all military platforms. The following CID development standards are offered by Young for consideration:

- Standardized data strategy and CID taxonomy
- Standards for data sharing/transmission
- Standards for databases
- Common algorithms for processing CID data and making CID determinations
- Common training for Joint and Coalition Force Operators in identifying battle space objects based on CID sources

d. **Effective CID Data Strategy**: A common data processing strategy where relevant data is apparent, trusted, interoperable, precise, timely and visible.

e. **Span Warfare Areas:** For maximum combat effectiveness surface, subsurface, space, and air resource assets must be integrated within the CID process.

f. **Increased level of Automation:** Future CID capabilities should focus on automating as many processes as possible. This will reduce the amount of variability that can be introduced into the system, inject higher levels of process efficiency, and ultimately shorten the detect/control/engage sequence.

g. **Isolate CID processes:** Utilize good sound OA design practices by modularizing and thereby isolating the CID process from other Combat System applications. This design principle reduces life cycle costs and supports technological insertion while minimizing adaptive component requirements. The benefits of this can also be realized during the test and

evaluation phase where CID sub-components, algorithms, and timing thresholds can be evaluated and analyzed separately to ensure optimal results are attained.

4. **Command and Control:** A Command and Control (C2) system for future aerospace warfare inevitably depends on NCW solutions. In "C2 System for Future Aerospace Warfare" (Young, 2004), Young describes that the C2 system's role is to optimize the resources both offensively and defensively to combat the aerospace threats. NCW-enabled C2 will enhance time-critical operational response by using the distributed warfare assets to select the best shooter from a set of geographically distributed firing units and to increase the chances of intercepting and eliminating multiple redundant shots to the targets. A prime example of collaborative C2 capability is the Integrated Fire Control (IFC) system.

Young further describes the Peer Computing Program (PCP), also known as the Integrated Architecture Behavior Model (IABM) that resides on each participating joint warfighting unit. The Joint SIAP System Engineering Organization (JSSEO) is using this program to develop a SIAP Distributed System concept to provide a NCW foundation for future joint C2 operations. The distributed SIAP system concept illustrated in Figure 7, involves multiple peers or PCPs acting together to provide interface interaction with the external non-SIAP entities within the operational scenario.

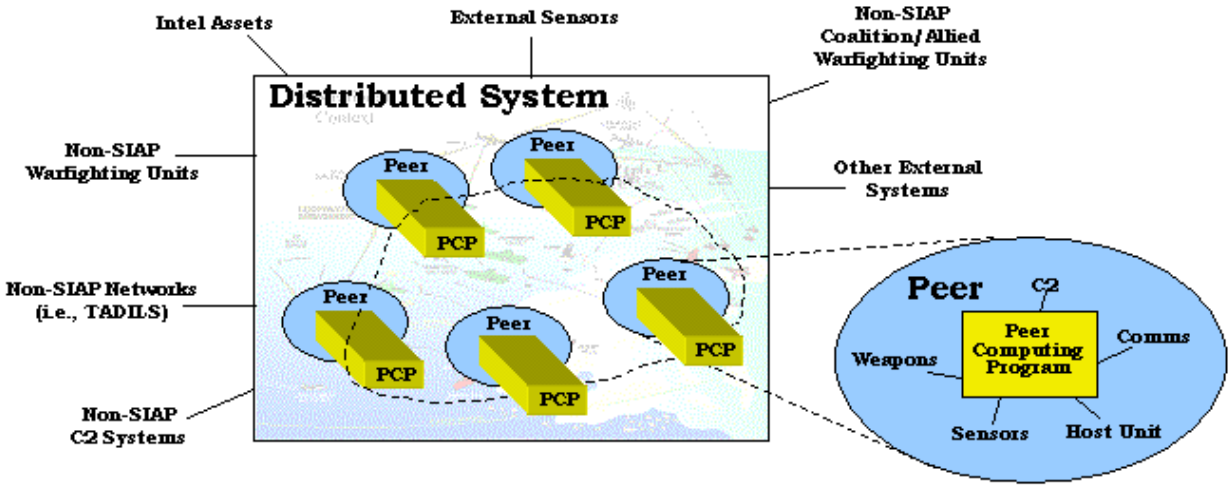

Figure 7. SIAP Distributed System Context Diagram (C2 System for Future Aerospace Warfare, Young, 2004)

Figure 8 further illustrates the manner in which each PCP-equipped unit employs the common processing methodology (identical computational and algorithmic methods) inherent to the SIAP philosophy.

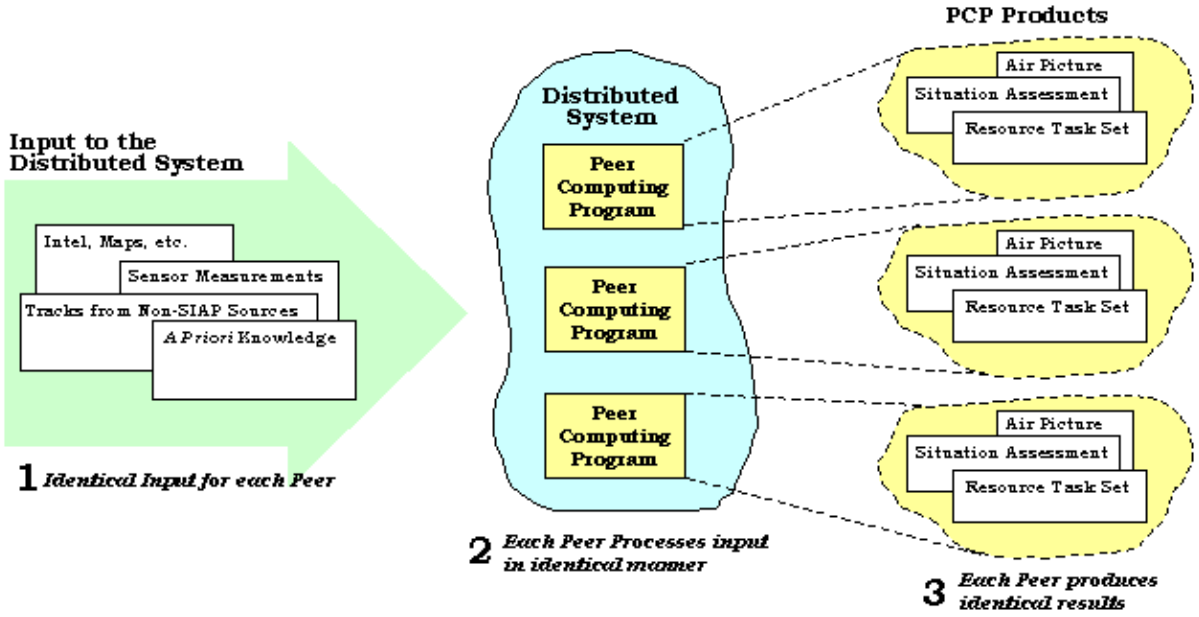

Figure 8. SIAP Common Processing Philosophy (C2 System for Future Aerospace Warfare, Young, 2004)

Core Peer Computing Program Capabilities: The core PCP capabilities function used to create the SIAP consists of common, continual and unambiguous tracks derived from real time and near real time data of airborne objects. The external interfaces of a single PCP unit are illustrated in the Figure 9, the PCP Context Diagram.

Information Architecture: The supporting information architecture required for SIAP is achieved through the establishment, maintenance and management of Peer-to-Peer (P2P) networks. A greatly improved situational awareness exists because of the netting together of information derived from these participating units. This unique collaboration involves a timely distribution, sharing, and integration of tactical information and warfare assets (sensors, weapons, warfighting units). Each participating unit uses the data fusion and tracking algorithms common to the PCP framework to take full advantage of raw data coming from the P2P communications network. An example of the SIAP Information Architecture concept is provided below (Figure 10).

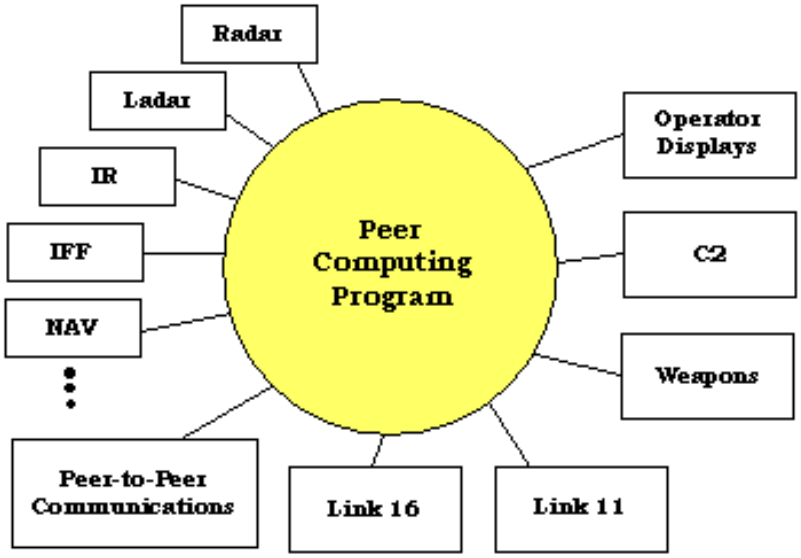

Figure 9. PCP Context Diagram (C2 System for Future Aerospace Warfare, Young, 2004)

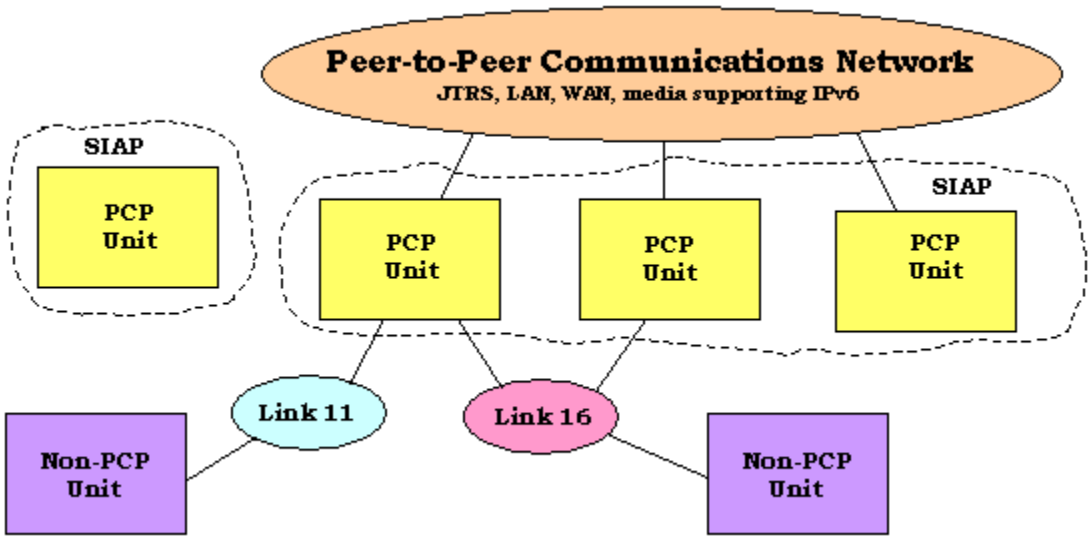

Figure 10. SIAP Information Architecture (C2 System for Future Aerospace Warfare, Young, 2004)

Transmission of large amounts of data in a timely fashion is required to support both the information architecture and a decentralized distributed Command and Control (C2), both of which are considered critical for NCW operation.

Concepts for Future Joint C2: The future joint C2 concept's basic premise is the philosophy of Common Processing where all PCP-equipped warfighting units will construct a common track picture from identically distributed data sets with common data processing and decision-making algorithms. These capabilities will build on the existing core SIAP PCP functions and will enable operation in an automated and coordinated fashion to produce identical Force-level decision recommendations. Figure 11 shows a diagram of a proposed future PCP functionality.

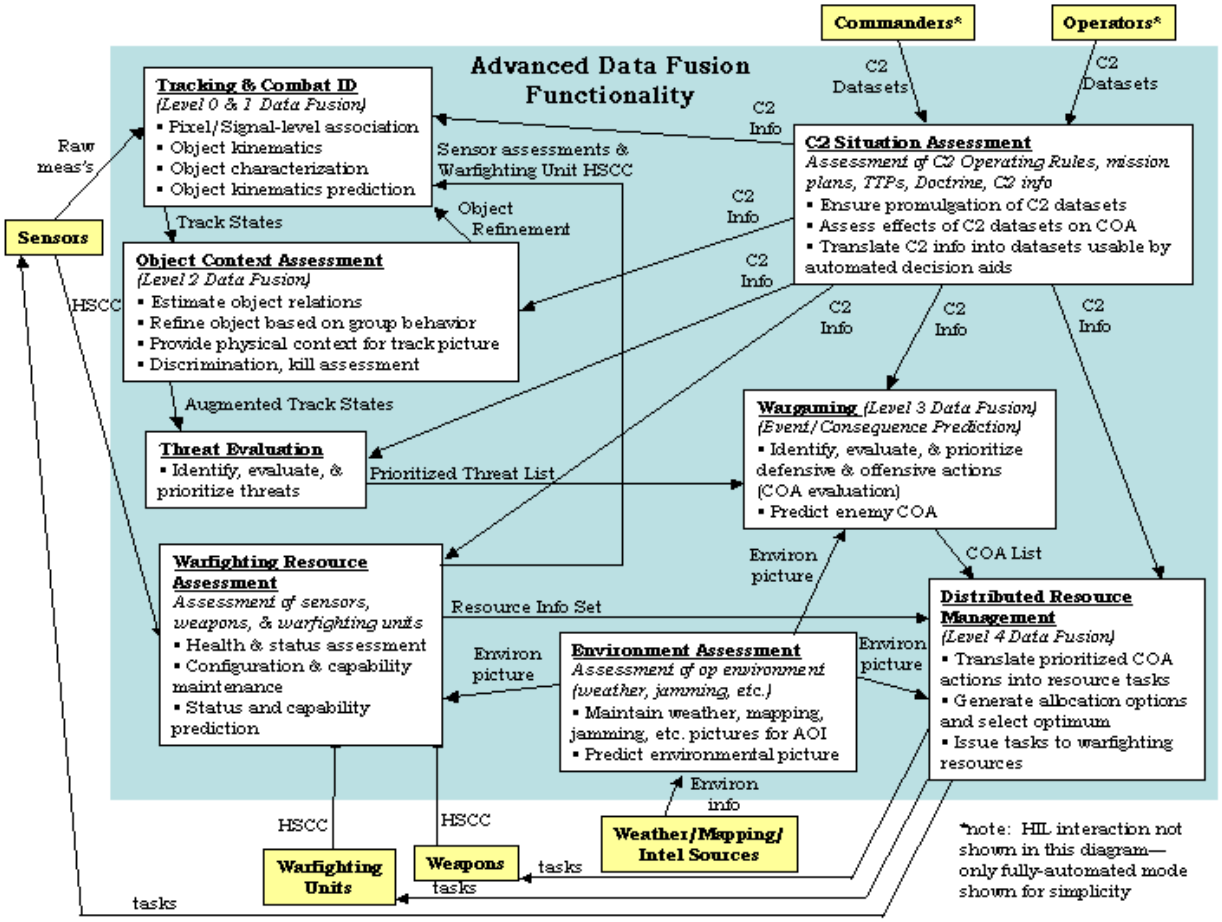

Figure 11. Future PCP Functionality (Young, 2004)

Advanced Situational Awareness/Assessment: The SIAP concept is based on a high level of situational awareness (SA), which is the ability of the collective peers to share a common understanding of the operational situation including the threat, the defended assets, the readiness of warfighting resources and the command and control

constraints. SA provides each peer with an accurate picture from a set of information that is updated on a continuous basis to most accurately reflect the real state of the battle space situation. The SA aspects of the operational situation include track picture, object context, threat picture, defended assets picture, warfighting resources, the environmental picture, and the C2 situation.

Situation Prediction/War gaming: Situation Prediction (SP) is identified as determining the potential impact of the Force's planned actions based on using a future prediction of the current situation to estimate the enemy course of action (COA). SP uses Automated Management Aids (AMA) to project enemy COA based on the real-time, near real-time and non-real-time operational situation. The SP function is comprised of Environmental Prediction, War-fighting Resource Projection, and War gaming or Event/Consequence Prediction.

5. Sensor Resource Management (SRM): "Naval Network-Centric Sensor Resource Management," (Johnson(Young)/Green 2002) describes the existing deficiencies associated with legacy Naval Battle Force sensor management and explores solutions for a network-centric sensor resource manager as a part of a Battle Force system of systems. SRM enables and optimizes the use of resources from the Naval Battle Force. Historically, the Navy has utilized a platform-centric foundation to independently address one mission area at a time. As more platforms were introduced, the complexity within the tactical environment increased and an effective management of Battle Force resources became crucial. This is to say, legacy system limitations have presented an enormous challenge. Cooperative sensor resource management is affected by legacy link formats and use of bandwidth and communication hardware. Existing architecture constraints do not provide for data distribution across the Battle Force to support SRM and NCW concepts. The Battle Force has to be considered from a network-centric and system-of-systems perspective to understand how commands and tasks can be executed. A lack of standardization in existing naval systems causes differences in commands and processes which ultimately translate into a lack of synchronization among the platforms.

Required Enablers for Cooperative SRM: Two key enablers to establish a Cooperative SRM are the establishment of a common synchronized Battle Force

information database and an automated link manager. As depicted in Figure 12, the three realms of the Battle Force Common Operational Picture (COP), Common Tactical Picture (CTP), and the Fire Control Picture (FCP) are synchronized into a Battle Force information database to achieve information superiority. By maintaining consistent situational awareness across the battle space, the Naval Battle Force establishes effective management of the threats and operations. The SRM concept includes managing sensors and networking resources from a decentralized platform perspective to maximize the area of coverage and accuracy of the data.

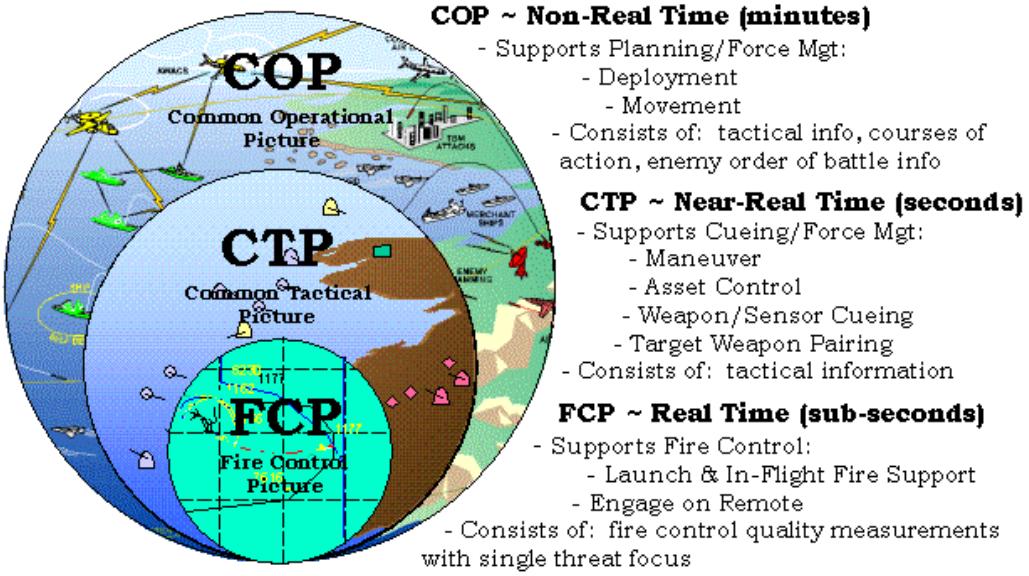

Figure 12. Three Realms of Battle Force Information (Naval Network-Centric Sensor Resource Management, Johnson/Green, 2002)

Automated control of data distribution throughout the Battle Force is an enabler of network-centric sensor management. The limitations of bandwidth can constrain the transmission and receipt of data among Battle Force platforms. The solution to effectively utilize bandwidth is to limit the distribution of data based on the current mission needs of the Battle Force. Figure 13 provides a representation of how this intelligent data distribution concept operates.

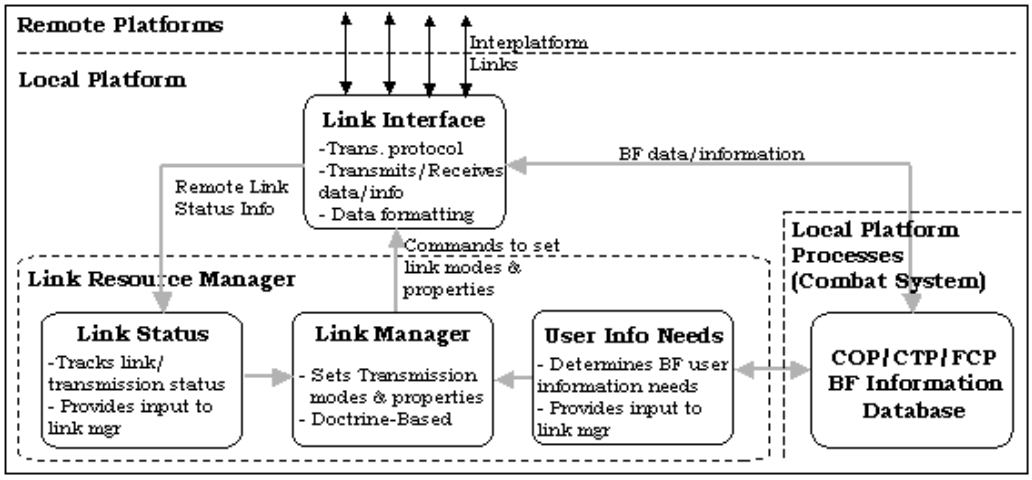

Figure 13. Intelligent Link Resource Management Concept (Naval Network-Centric Sensor Resource Management, Johnson/Green, 2002)

The automated and distributed resource management system places a link manager at each decision node. This link manager maintains tracks, determines feasibility and need for transmission, then issues mission-related commands to other link managers and transmits data as required.

Benefits of Cooperative SRM: It is expected that the following advantages may be realized from the implementation of network-centric sensor resource management:

a. An increase in target tracking accuracy across the battle space
b. A decrease in degraded surveillance zones
c. An increase in the detection range of the Battle Force
d. A decrease in the average Battle Force reaction time
e. Enable better utilization of sensor assets
f. Enable greater remote engagement capability resources

The essence of Naval Network-Centric Sensor Resource Management is that it will enable information superiority by allowing earlier decisions to be made based on more accurate data and faster responses from the warfighters within the Battle Force.

C. EARLY OPEN ARCHITECTURE INTERPRETATIONS

"OA the Critical NCW Enabler" (Rushton, First Edition, dated March 18, 2004) sets the stage on why OA is imperative to attaining full enablement of our wartime potential in the Network Centric Warfare (NCW) arena. Through a close examination of the threats and environments the Navy was challenged with defending in the past, Rushton helps us in understanding the different challenges that we face now. There is a compelling case for OA, stating that rapid, technological globalization demands that we utilize NCW and embrace OA to successfully combat present and future asymmetric terrors. The technical conditions needed to fully achieve joint interoperability, network sensor assets, and ensure information is seamlessly shared, demands the adoption of OA. Rushton provides guidance, motivation, and justification for the work accomplished by this thesis. That being said, we will reiterate some of his commentary to capture some key fundamental concepts that were used as a basis for this research project.

Historically, tactical combat system capabilities were designed to defend against the "blue water" threats associated with the Cold War. Namely, integrated fire control systems were platform-centric in that they were Point-to-Point, closed, tight-looped systems, co-locating sensors with weapons, operating to minimize the time from sensor detection, to command and control, to weapon engagement. As the Cold War passed, technology evolved at an unprecedented rate, rendering the tactical weapon systems of US Navy ships unaffordable to maintain. DoD realized the phenomenal potentials associated with Internet Protocol (IP) based systems. Additionally, the battle space continuum now involved threats in the littoral region, threats often masked from platform co-located sensors and weapons. The Navy, seeing they were ill equipped to meet the new challenges, expanded its requirements base and developed FORCEnet concept of operations. FORCEnet bases it foundation on a shared implementation of a global information network and its framework on OA system design principles, standards, and architecture. OA enables a new approach that exploits open systems and Commercial Off-The-Shelf (COTS) integration, allowing for easier management of technology insertion through reusable adaptive software components.

OA systems employ two fundamental elements: a technical architecture defined by the standards and guidance set forth in the OA Computing Environment (OACE) Technologies and Standards (NSWC, Dahlgren Division, 04 Sept 2003) and a "functional architecture embracing of an agreed upon framework of functional allocations, common/standard applications and services". Criteria for OA compliant categories have been developed and are defined in Figure 14 below:

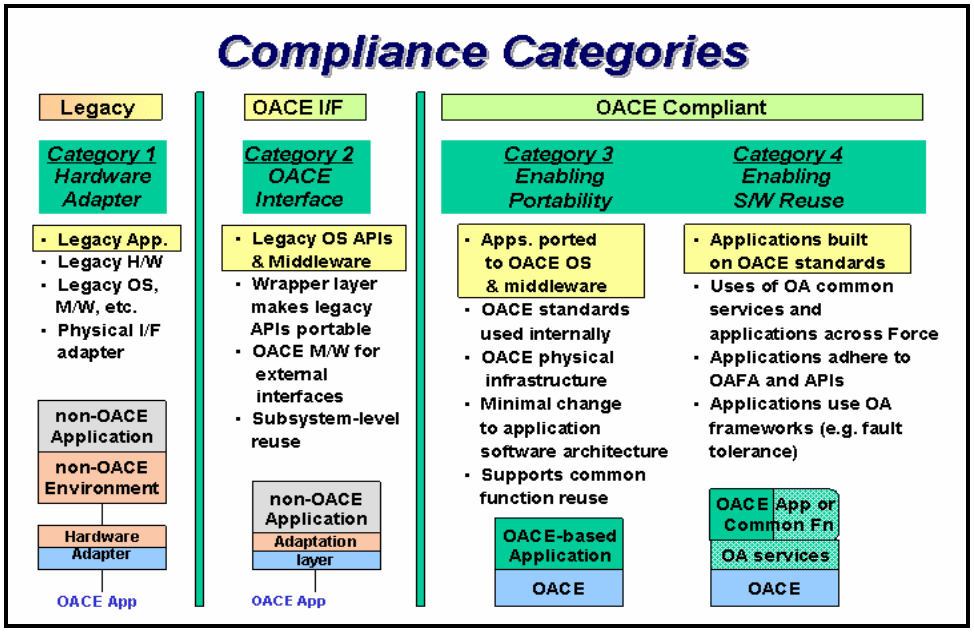

Figure 14. OA Compliance Categories (OACE Technologies and Standards, NSWC, Dahlgren Division, 04 Sept 2003)

The majority of today's combat systems are Categories 1 and 2, non-modularized systems where the hardware and software is coupled. SSDS MK2 MOD 3B will be the first OA Category 3 compliant system, meaning the software is not constrained to the hardware infrastructure. SSDS MK2 MOD3B is currently in its final development stages. Category 4 will implement common services and applications such as correlation/de-correlation algorithms, threat identification rankings and cross-platform track management. The OACE is based on a commercially modeled principle that separates and decouples hardware and software, see Figure 15. While its benefits and design, are well documented, developed, and understood, the OA functional architecture may not.

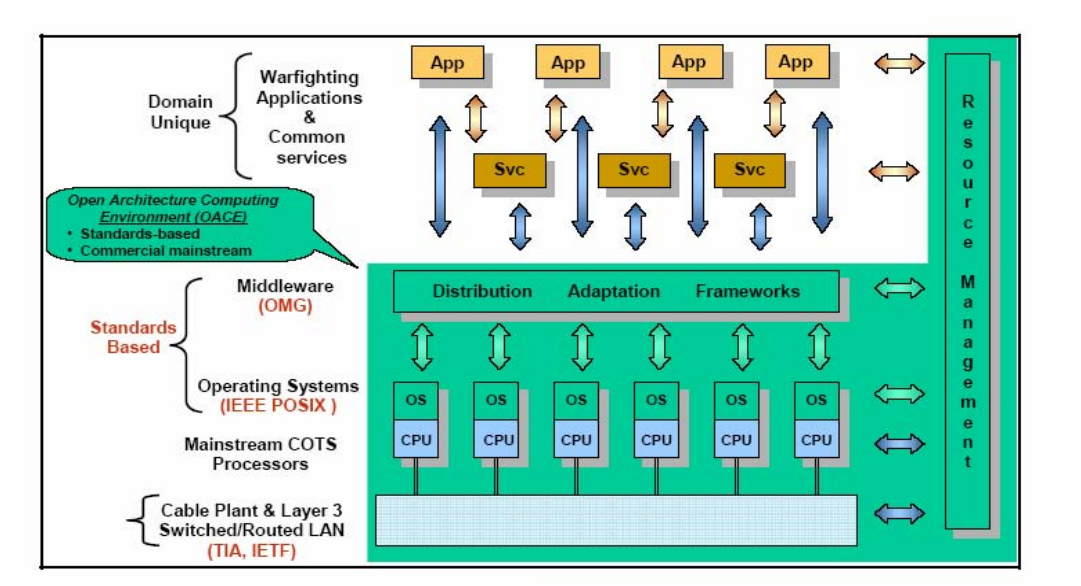

Figure 15. OA Computing Environments (Open Architecture in Naval Combat System Computing of the 21st Century, Strei, 2003)

The OA functional architecture provides the characterization and functional framework for enabling optimal networked warfighting capability. It partitions the OA system into functionally logical modules from a Combat Systems perspective while reducing duplication and eliminating service-specific related objects. The guiding functional principle is to construct a system which can be installed on any FORCEnet unit and when operational will seamlessly network with other OA participating units, sharing sensors, INTEL data, managing tracks, weapon resources and fire control solutions. The effort will achieve a uniform common operational and command and control picture, one that is fully optimized for the warfighter. Rushton also offers us the PEO IWS OA Functional Domain Model, but does not delve further into its functional constructs. He does state however that a common agreement must be made regarding common servicing of time, navigation, data registration, and the establishment of a core, common, joint track manager application. Successful joint network-centric decision-making, Common Identification (CID) and IFC are all premised on precise and timely track reporting and cohesion of the operational picture.

One clear objective of Open Architecture (OA) is to enable faster insertion of new technologies and systems with less complexity to produce superior and more affordable weapon systems. Similar to the Rushton concept, "Open Architecture in Naval Combat System Computing of the 21st Century," (Strei 2003) provides insight into a possible OA implementation in FORCEnet. Strei proposes that using non-proprietary COTS technologies along with commercial standards for products, specifications, and standards will allow greater reuse of computer programs and a broader vendor base upon which to draw.

The Challenge of Accelerating Computing Technologies: Acceleration in computing technologies started after the launch of Sputnik by Soviet Union in 1957. New U. S. defense requirements and virtually an unlimited budget at that time set the pace for the development of custom-designed computer hardware and tightly coupled software due to unavailability in the commercial or civilian sectors.

In the 1980s, the computing requirements in the commercial and civilian sectors resulted in unprecedented innovation and product development in commercial marketplace. Increase in demand for information technology and systems in the commercial marketplace caused the prices to fall due to advent of low-cost, high-performance microprocessor chips and associated hardware. These developments caused the custom-designed military computer and system to fall behind their commercial counterparts in fundamental capabilities and economies of scale.

An Integrated Warfare Approach: The PEO IWS approach is to maximize fundamental commonality and interoperability across warships, aircraft, weapons, sensors and basically any defense program. To achieve this, PEO IWS architecture requires consolidation of Navy computing systems into a single open-system emphasizing common “core” computing architecture and standards and deriving a warfare systems functional architecture within the OA. This approach mirrors the approach upon which this project is based.

The Navy OA program will develop and evolve common warfare applications, services, and computing resources all in a single implementation cycle rather than independently across multiple programs. These also require adoption of open commercial

information system technology standards and non-proprietary standard interfaces, services, and formats that are available on mainstream COTS system. The portability, scalability, extensibility, and flexibility are key metrics to be included in the Navy OA program.

The PEO IWS OA program has fielded an Engineering Development Model (EDM), the first of which is an open Aegis system that runs on the OACE and contains selected common and specialized warfighting services and applications. The notional EDM open system architecture illustration (Figure 16) defines the relationships between the commercial and defense industry general and domain-unique hardware, middleware, and software.

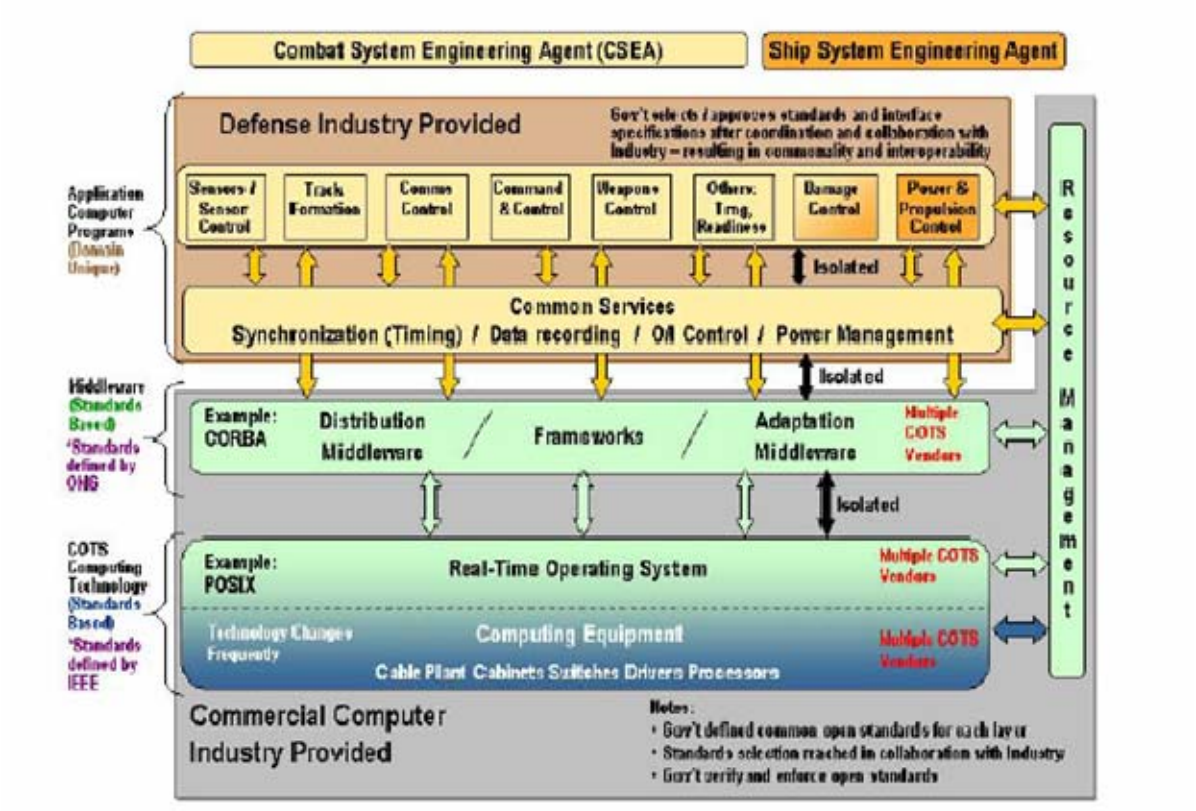

Figure 16. Notional Open System Architecture Strei, 2003.

In addition, the Navy OA program will take advantage of other Navys, and services, and OA initiatives that have been pioneered in several Naval Departments such as the Virginia (SSN 774) class nuclear-powered attack submarine program and Acoustic Raid COTS Insertion (A-RCI).

Summary: A solid FORCEnet OA implementation strategy has been laid out over the course of the last several years as shown in this literature review. Simple, easy to understand, well-defined system partitions and boundaries are essential for successful implementation. Interfaces must be based on established commercial practices and COTS hardware. The progress made in earlier efforts, in particular with respect to PEO IWS, will not be repeated in this project. The intent is to build off what has been done to date in the development of specific engagement scenarios, and to revise the PEO IWS OA architecture based on a lower level implementation.

THIS PAGE INTENTIONALLY LEFT BLANK

III. ANALYSIS

A. CHARACTERIZATION OF THE BATTLE SPACE

The basic operational concept of FORCEnet Open Architecture (Fn/OA) is to pair threats with ideal weapons using all available sensors and assets from platforms operating within the Battle Force network. As originally illustrated in the Three Realms of Battle Force Information (Figure 12), this pairing of targets and weapons will occur in three different time domains: the COP, CTP, and the FCP. Each time domain is a subset of the higher level as shown in a mockup of a SIAP in Figure 17. The COP is the situational awareness view at the Commander-In-Chief (CINC) level. "The CTP is a clear, consistent, and intuitively obvious display of all Real-World Objects (RWOs) of interest to users across the force within an operator selectable region of interest" (Luessen, 2003). The SIAP is a subset of the CTP.

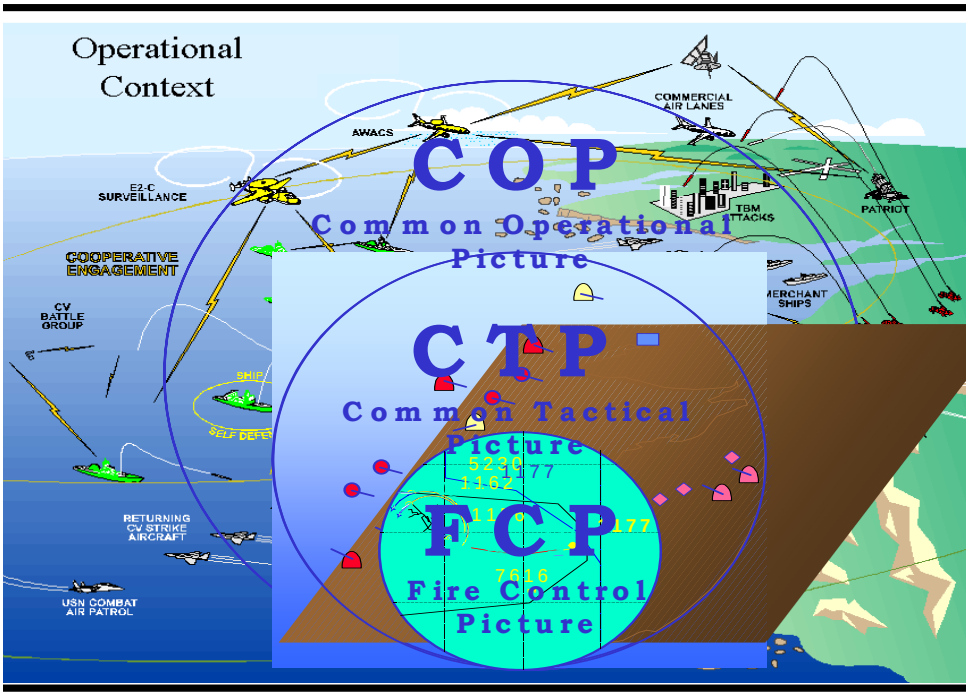

Figure 17. FORCEnet Operational Content (Johnson/Green 2002)

The FCP is the platform-centric situational awareness view that may be shared among others in the Expeditionary Strike Group (ESG) or the Carrier Strike Group (CSG). Tracks can be obtained from one or more platforms, and cued to other platforms within the ESG or CSG. The track will receive Combat Identification (CID), and will be labeled unknown, assumed friend, friend, suspect, hostile, or assumed hostile. All CID tracks will eventually reside in all three domains. The sensing platform will place the track in the FCP. After CID, the track may be cued to other platforms within the group, or may be added to the CTP through the Local Area Network (LAN). Finally, the CID track will be added to the COP using legacy systems such as Global Command and Control System Maritime (GCCS-M), Link 11, Link 16, Cooperative Engagement Capability (CEC), Wide Area Network (WAN) or with new systems such as the Global Information Grid (GIG).

Threats will be evaluated and strategies established based on functionality available on all platforms within the CTP. Threats will be prioritized based on the present situational awareness and the predicted enemy COA. The system will then assess the environment and warfighting resources available, and match the resources to the prioritized threat (Young, 2004). More than one platform may be involved in an engagement including both surface and air platforms. If an engagement is assigned to multiple platforms one of the following three techniques will be used to counter the threat (Young 2004):

1) Engage on Remote (EOR)
2) Forward Pass (FP)
3) Remote Fire (RF)

Process depictions and Functional Flow Block diagrams are provided below for each of the three selected mission concepts.

1. Engagement Types

a. Engage on Remote (EOR): Remote data is used to support all engagement phases of a locally launched missile. In this scenario, a remote platform passes tracking and engagement information to the local platform. The local platform

launches the weapon using non-organic sensor source data. The remote platform then supports the weapon throughout flight as necessary (command midcourse guidance or similar). If the weapon has an active seeker, it may switch to inertial midcourse guidance in-flight and finish in terminal guidance through intercept without support from either platform. An active weapon can switch between active and semi-active operation. Figure 18 provides a depiction of the dynamics involved in this particular mission, while Figure 19 provides the proposed Functional Flow Block Diagram.

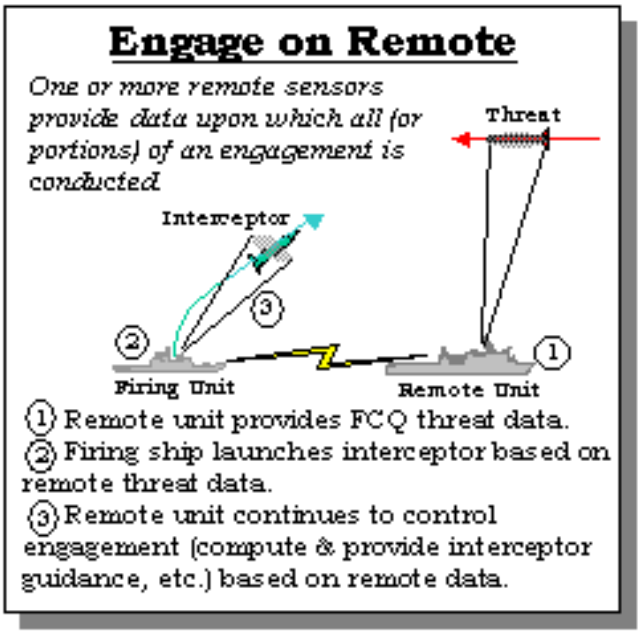

Figure 18. Engage on Remote Mission Concept (Young 2004)

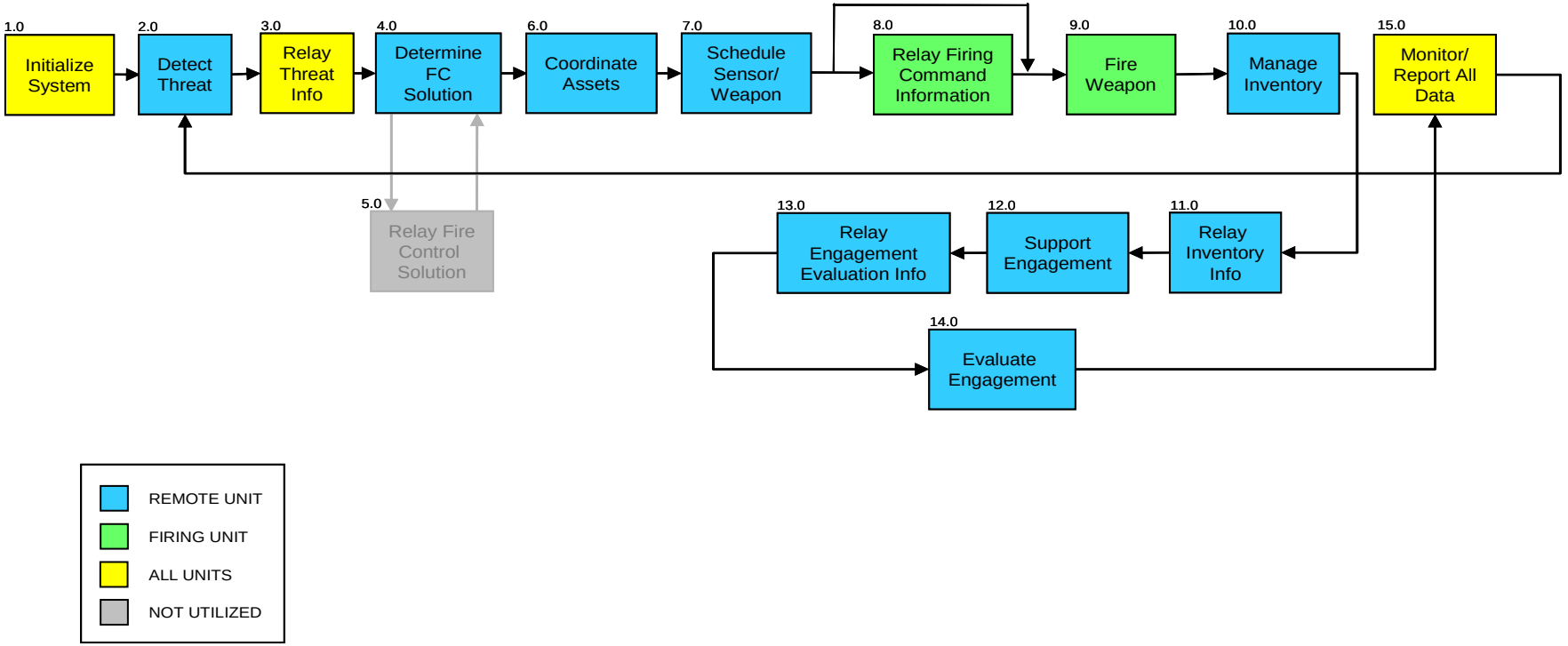

Figure 19. Engage on Remote FFBD

b. Forward Pass (FP): Control of an in-flight missile is handed off to another unit to complete the engagement against a threat. In this scenario, a platform launches a missile from local inventory using organic track data. The launching platform then passes control of the in-flight missile to another unit to support the engagement throughout the remainder of the flight. The unit taking control of the in-flight missile will support the engagement using command midcourse guidance or terminal guidance as required. Figure 20 provides a depiction of the dynamics involved in this particular mission, while Figure 21 provides the proposed Functional Flow Block Diagram.

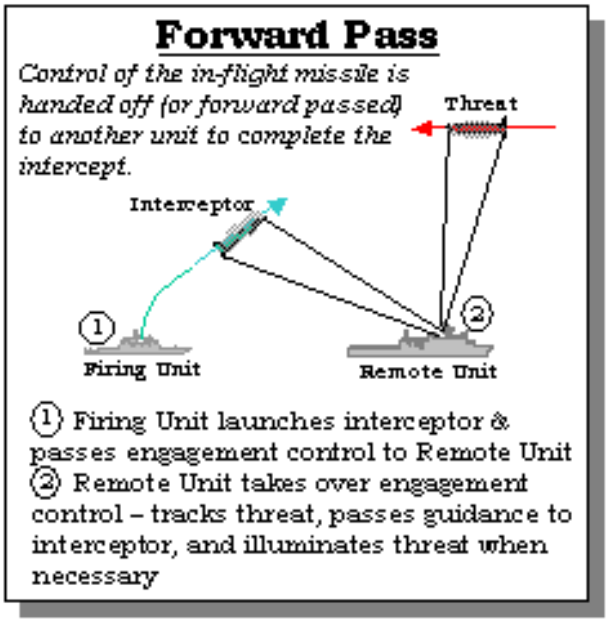

Figure 20. Forward Pass Mission Concept (Young, 2004)

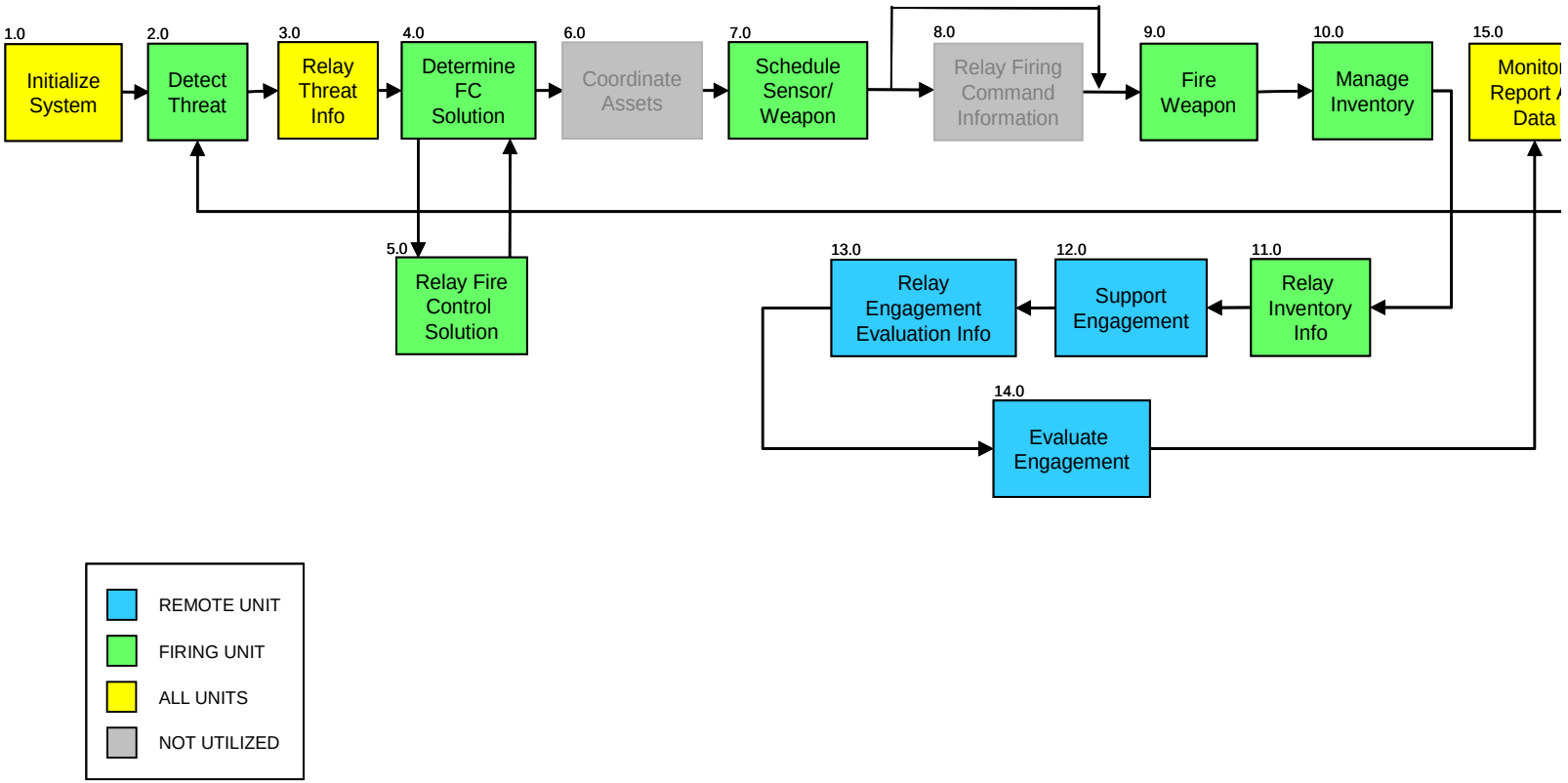

Figure 21. Forward Pass FFBD

c. Remote Fire (RF): A remote unit makes a missile launch decision and either the remote unit or local unit can support the in-flight missile until the engagement completes. The remote platform passes launch data and firing orders to the local platform. The local platform launches the weapon and then either supports the weapon throughout flight using command midcourse guidance or terminal homing phase as required. If the weapon has an active seeker, it may switch to inertial midcourse guidance in-flight and finish in terminal guidance through intercept without support from either platform. Figure 22 provides a depiction of the dynamics involved in this particular mission, while Figure 23 provides the proposed Functional Flow Block Diagram.

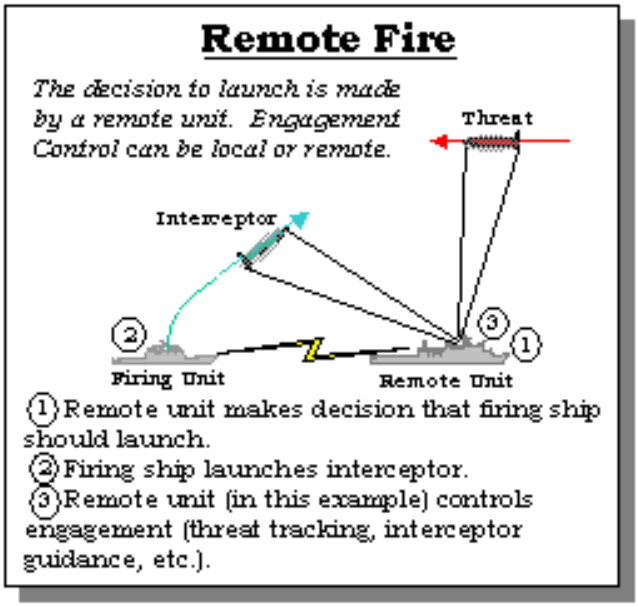

Figure 22. Remote Fire Mission Concept (Young, 2004)

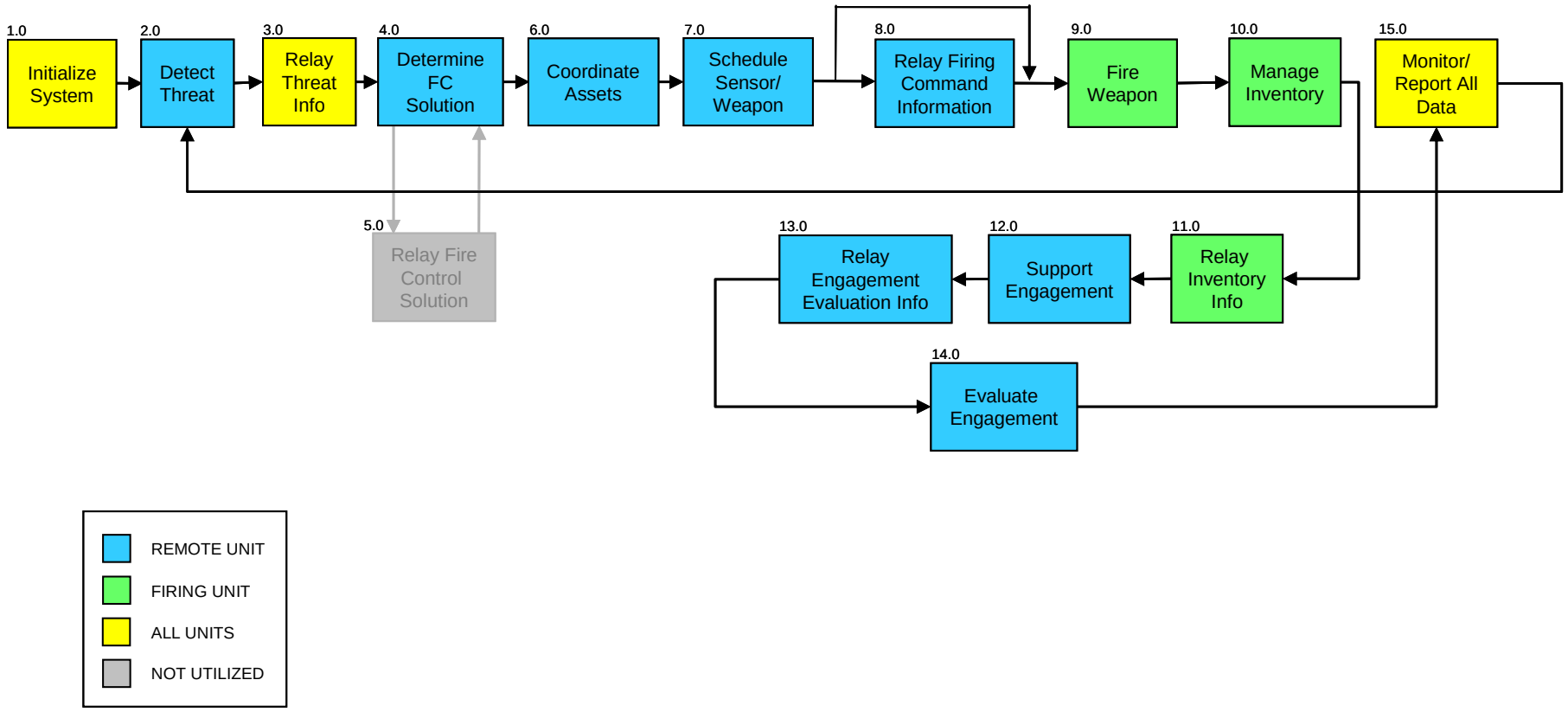

Figure 23. Remote Fire FFBD

2. Enabling Capabilities Required: The following provides a list of the capabilities necessary to conduct the selected engagement scenarios:

a. Current Systems

1) Aegis Cruiser and/or Destroyer with Integrated Fire Control (IFC) capability.
2) Advanced Hawkeye
3) An active or semi-active weapon with command mid-course guidance, inertial midcourse guidance and link capability that supports (IFC).
4) Peer to peer communications network that supports Link 11, Link 16, CEC, UHF, EHF, SHF, and HF.

b. Future Systems

1) CG(X) and/or DD(X) with Integrated Fire Control (IFC)
2) An active or semi-active weapon with command mid-course guidance, inertial midcourse guidance and link capability that supports (IFC).
3) Peer to peer communications network that supports Link 16, GIG, UHF, EHF, SHF, and HF.
4) Advanced data fusion functionality

B. DESIGN PRINCIPLES APPLIED

This project used the PEO IWS OA Domain Model along with "FORCEnet Implementation Strategy" (NRC 2005) as the initial starting point to begin the systems engineering process. It was determined early on in the process that FORCEnet system development was already beyond the concept development phase and required an unconventional approach. Various contractors and government activities have already settled on a high level operational architecture for the system; consequently this effort began at a point in the development cycle past the preparatory tasks laid out in The Engineering Design of Systems (Buede 2000). The project employed a top down approach by decomposing the IWS OA Domain Model, two levels, applying three specific detect-control-engage scenarios at the root levels, and recomposing the process

path to formulate a unique OA Domain Model in a bottom up approach. Specific system development activities were employed as follows:

1) Original Problem Analysis and Reference Data Collection
2) Layout Operational Views
3) Requirements Analysis
4) Requirements Allocation
5) System Decomposition
6) FFBD Development
7) Simulation Model Development
8) System Re-composition
9) Comparison Analysis
10) Compilation of Results
11) Conclusions and Recommendations

Once the original problem statement was reviewed and understood, Operational View (OV) diagrams were developed for each specific scenario. These OVs are provided in Appendix A. System decomposition and requirements analysis were conducted in parallel. As the system was decomposed, derived requirements were identified and developed. With this, methods of system decomposition were sometimes altered and several iterations of both processes were required.

1. REQUIREMENTS ANALYSIS: A general set of mission and originating requirements was provided in the original problem statement (Blanchard-Fabrycky, 2000). As the system was decomposed, additional derived requirements were developed. Detailed engineering statements based on these requirements were compiled as follows:

Integrated Fire Control (IFC) Scenarios

1) Engage on Remote (EoR)

2) Forward Pass (FP)

3) Remote Fire (RF)

Requirements Common to All Scenarios:

a) Firing Unit (FRU) receive Fire Control Quality (FCQ) data on threat from Remote Unit(s) (RUs).

b) Validate FCQ data, enable FRU to act.

c) Maintain Common Operational Picture (COP) of local tracks.

d) Develop Fire Control Solution (FCS) based on FCQ data.

e) Correlate FRU FCS with RU FCS.

f) Resolve differences between FRU and RU FCSs.

g) FRU override opposing FCS on authorization.

h) Approve engagement.

i) FRU and RU send, receive, and update weapons inventory.

j) FRU and/or RU send, receive, and update engagement status.

k) FRU and/or RU send, receive intercept information.

l) FRU, RU and Interceptor correlate illumination and link frequencies.

Overarching Requirements:

a) Build common database algorithms to store widely shared information.

b) Implement standard use interfaces to access information;

Scenario Specific Requirements:

Engage on Remote

a) FRU launch applicable weapon based on validated FCQ, correlated or overridden FCS, and approved engagement.

b) FRU support Mid-Course Guidance (Link or Self Destruct Timer Reset).

c) FRU, RU or Interceptor provides target illumination.

d) RU send intercept information.

e) FRU receive intercept information.

f) Update COP.

Forward Pass:

a) FRU launch applicable weapon based on validated FCQ and approved engagement.

b) FRU and RU acknowledge handoff.

c) FRU and RU support portions or all of Mid-Course Guidance (Link or Self Destruct Timer Reset).

d) RU or Interceptor provide target illumination.

e) RU send intercept information.

f) FRU receive intercept information.

g) Update COP.

Remote Fire:

a) FRU launch applicable weapon on approved orders from RU.

b) RU support Mid-Course Guidance (Link or Self Destruct Timer Reset).

c) RU or Interceptor provide target illumination.

d) RU send intercept information.

e) FRU receive intercept information.

f) Update COP.

2. REQUIREMENTS ALLOCATION: Requirements were allocated to the notional functional blocks of the IWS OA Domain Model. This task was undertaken with the knowledge that the allocation may change once the decomposition was complete, FFBDs were developed and simulation results made available. The requirements allocation resulted in the following functional block definitions:

SEARCH and DETECT (S/D) [1]

DESCRIPTION: The S/D functional component will utilize local sensors to detect contacts. Sensor track positional reports and INTEL reports will be distributed over the LAN for other users. S/D will accept track cues from other remote units and task local sensors to search and detect for possible threats.

INPUTS: Accept data from functional blocks 2 and 6.

OUTPUTS: Sensor track and INTEL positional reports

REQUIREMENTS:

1. Each Force-Net unit shall make local sensor data available to other units in near real time accuracy.
2. Each Force-Net unit shall make INTEL data available to other units in near real time accuracy.
3. Use Intel sources and other sensor information to provide tracking cues to remote surveillance sensors.
4. Accept tracking cues from remote units.
5. FRU shall support Mid-Course Guidance (Link or Self Destruct Timer Reset).
6. FRU, RU or Interceptor shall provide target illumination

DATA INFORMATION SERVICES (D/S) [2]

DESCRIPTION: The D/S functional component will maintain all time-critical system track data for real time (RT) and non-real time (NRT) tracks, including kinematics, identification, class, Link-Track Number, and primary and secondary source information. D/S will distribute time critical track data over LAN for other users.

INPUTS: Accept data from functional blocks 1, 3, and 6

OUTPUTS: Track Attribute data.

REQUIREMENTS: Track parametric data

1. Implement common processes for guidance computation and engagement control

2. Ensure participation and coordination of multiple non-collocated warfare assets
3. Store and maintain common system track data (RT and NRT), including best and supporting sources in near real-time accuracy.
4. Perform sensor tasking based on shared knowledge of battle space, including knowing capabilities and locations of all participating sensors
5. Classify tracks based on IFF and INTEL data.
6. RU shall send intercept information
7. Shall update COP.

PLANNING ASSESSMENT and DECISION (PAD) [3]

DESCRIPTION: The PAD functional component will direct execution of all of the various warfare areas, perform threat assessments, and accept Command and Control orders.

INPUTS: Accept data from functional blocks 2, 4, 6, and 8.

OUTPUTS: C2 event and mission planning

REQUIREMENTS:

1. Provide for automated best resource selection decisions to select the best shooter.
2. Provide for automated best resource selection decisions to predict which sensors can best generate fire control quality data throughout engagement.
3. Provide for automated best resource selection to determine which units are capable of accepting control of an engagement after launch to enable forward pass.
4. Develop fire control solutions from FCQ data and information provided by one or more non-organic sensor sources.
5. System shall correlate FRU FCS with RU FCS.
6. Allow for FRU over-ride opposing FCS on authorization.
7. System shall approve or disapprove remote engagements.

8. FRU and/or RU shall send, receive, and update engagement status
9. FRU, RU and Interceptor shall correlate illumination and link frequencies.

WEAPON ASSET SERVICES [4]

DESCRIPTION: controls and coordinates all shipboard and shipboard-controlled assets included in the mission execution block

INPUTS: Accept data from functional blocks 2, 3, 5, and 6

OUTPUTS: Weapons scheduling

REQUIREMENTS:

1. Defend against significant number of aerospace targets
2. Support the manual selection and control of warfare assets during an engagement
3. Direct distributed warfare resources in a collaborative manner
4. Ensure participation and coordination of multiple non-collocated warfare assets
5. Firing Unit (FRU) shall receive, process and maintain Fire Control Quality (FCQ) data on the threat from Remote Unit(s) (RUs).
6. Firing Unit shall validate FCQ data.
7. Firing Unit shall enable FRU to act on threat.
8. FRU and RU shall send, receive, and update weapons inventory

MISSION EXECUTION [5]

DESCRIPTION: Maintains all weapons, remote vehicle, ship and communications assets.

INPUTS: Accept data from functional blocks 4 and 8

OUTPUTS: Status of ship assets and equipment

REQUIREMENTS:

1. Ensure participation and coordination of multiple non-collocated warfare assets

2. Provide mid-course guidance to interceptors by units other than the launching unit

3. Conduct engagements based on fire control solutions from information provided by one or more non-organic sensor sources

4. FRU and/or RU shall send, receive intercept information

5. FRU shall launch applicable weapon(s) based on validated FCQ, correlated or overridden FCS, and approved engagement

EXTERNAL COMMUNICATIONS [6]

DESCRIPTION: represents the link between the combat system and the various data sources within and external to Battle Force; responsible for sending/receiving track data, mission plans, intelligence to and from other units in the Battle Force.

INPUTS: Accept data from functional blocks 2, 3, 4, and 6

OUTPUTS: Network formatted tracking and mission related data

REQUIREMENTS:

1. Transmit, Receive and Forward all data exchanged between Force Level and Unit Level.

COMMON SERVICES [7]

DESCRIPTION: represents all services within the Combat level, Unit or Battle Force Level that are common.

INPUTS: Accept data from all functional blocks

OUTPUTS: Environment, Time, Intel database

REQUIREMENTS:

1. Share real-time target information and eliminate correlation errors

2. Maintain Common Operational Picture (COP) of local tracks.

FORCE PLANNING and COORDINATION [9]

DESCRIPTION: Provides mission coordination at the Battle Force level; processes Force Orders; assesses the mission plan and provides re-planning as needed.

INPUTS: Accept data from functional blocks 6

OUTPUTS: Force and Joint level mission schedules

REQUIREMENTS:

1. Provide mid-course guidance to interceptors using externally provided information

3. DECOMPOSITION/RE-COMPOSITION: The decomposition and re-composition process results in a unique OA Domain Model for comparison to the IWS OA Domain Model. Furthermore, the process facilitated in-depth analysis that provides observations, conclusions and suggestions that may be used in the future to develop the physical architecture for FORCEnet OA. The initial phase of this project utilized additional systems engineering processes as tools to aid in preliminary developmental efforts. These tools are identified below:

a) As described in Engineering Design of Systems (Buede, 1998), Integrated Definition for Function (IDEF) modeling was first employed for decomposition and is provided in Appendix C. A-0 External Systems diagram, and A0 First level decomposition proved to be useful as the analysis progressed, but were not used in the final result.

b) Since all networks exchange data, the data context and data flow diagrams described in Process for System Architecture and Requirements Engineering (Hatley-Pirbhai, 2000) were developed and are provided in Appendix A. These diagrams also proved to be useful as the analysis progressed, but were not used in the final result.

4. SIMULATION MODELING: Since FORCEnet is a system of data flows between Battle Force platforms, the problem statement should address concerns over data latency between the data distribution levels within the Fire

Control, Tactical, and Common Operational Pictures (Figure 17). Furthermore, there is concern that allocated system bandwidth will ensure time critical data rates are achieved. This is critical to proper system performance. Queuing processes must also be monitored during periods when the system is heavily loaded to avoid gridlock. Individual platform connectivity to the system will also impact performance. The system must degrade gracefully when and if platforms drop off the network and remain stable as platforms reconnect. Simulating a functioning operational system using a computer-generated model allows the actual system to be evaluated based on various data flow rates as well as gridlock and connectivity concerns. A commercially available simulation software application, Arena®, was used to validate the system design, and evaluate the impact of design parameter variation.

C. CONCEPTUAL DESIGN

1. Functional Flow Block Diagrams

The design principles (Section II) used for EoR, FP, and RF scenario development are based on detailed first and second level decompositions that identify each sub-function that is required to conduct an engagement. These detailed first level FFBDs are shown again below. Each of the three scenarios are described in Section II. Analysis of the resulting individual FFBDs identify similar sub-functions that could be for any of the three scenarios. From a data processing and data fusion perspective, all three scenarios will process in a similar fashion. Differences in processing will arise when determining what platform will perform what function. In the detect-control-engage sequence, multiple platforms may be qualified to perform any one of these three functions, and multiple handoffs could be made as the Fire Control, Common Tactical, and Common Operational Pictures update. Processing and assigning would be handled separately, and updated frequently as changes in the battle space continuum occur. An in-flight weapon is particularly flexible when operating in inertial (autonomous) midcourse mode rather than command midcourse mode, and could be easily handed off to various platforms operating in the battle space. This flexibility is captured in the sub-function FFBDs described below in Figure 24 through Figure 37.

Conceptual Design Sub-Function FFBDs

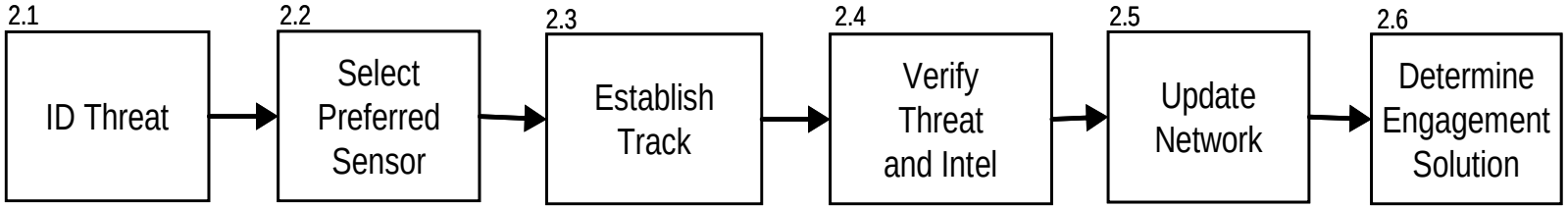

Figure 24. Detect Threat

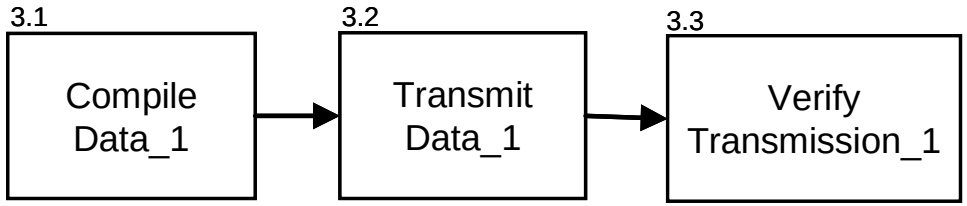

Figure 25. Relay Threat Information

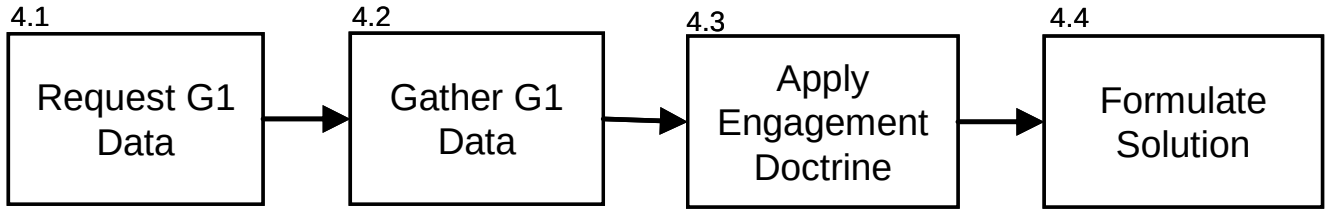

Figure 26. Determine Fire Control Solution

Conceptual Design Sub-Function FFBDs (Continued)

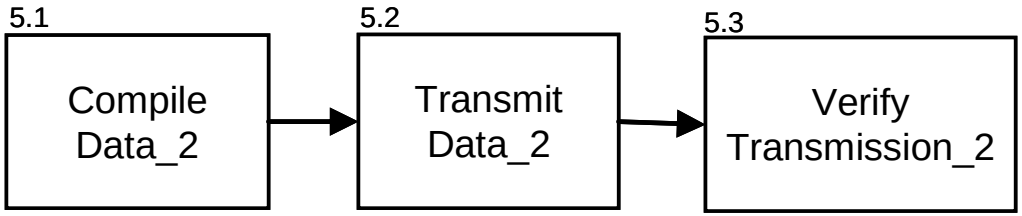

Figure 27. Relay Fire Control Solution

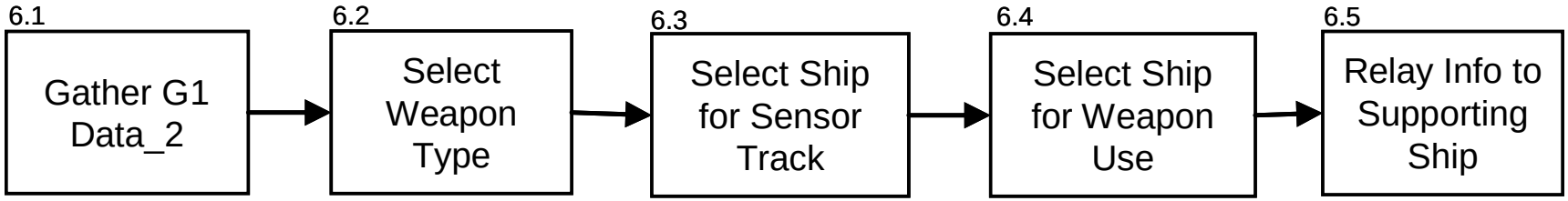

Figure 28. Coordinate Assets

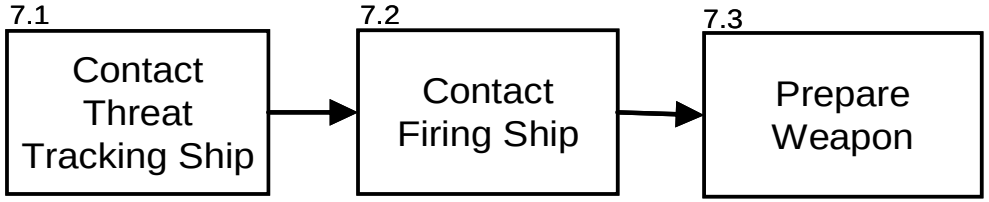

Figure 29. Schedule Sensors/Weapon

Conceptual Design Sub-Function FFBDs (Continued)

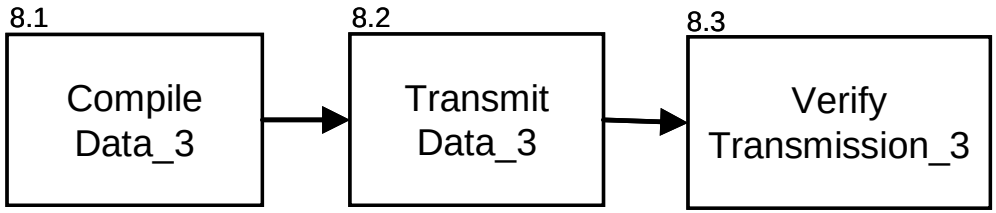

Figure 31. Relay Firing Command Information

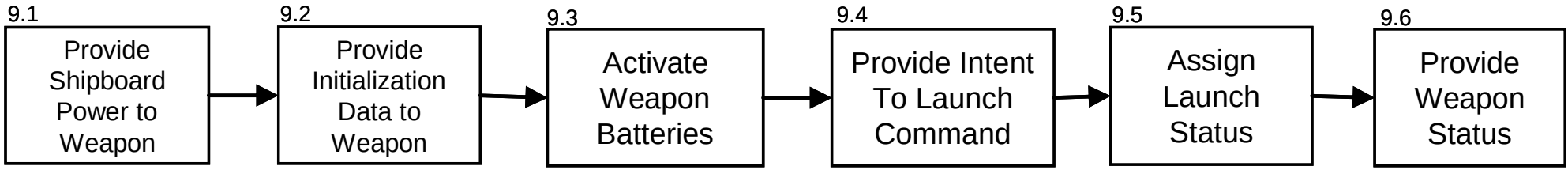

Figure 32. Fire Weapon

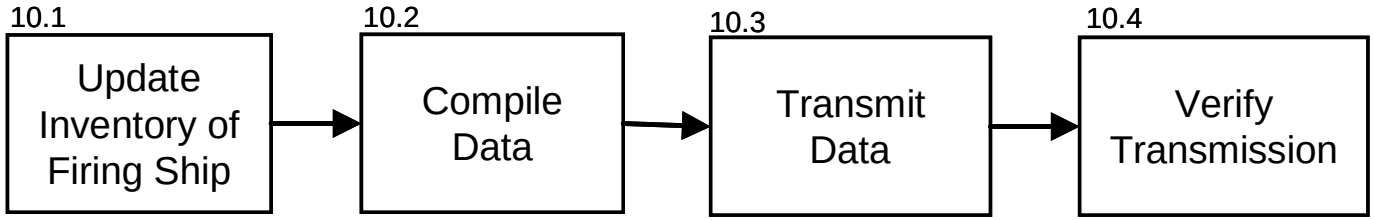

Figure 33. Manage Inventory

Conceptual Design Sub-Function FFBDs (Continued)

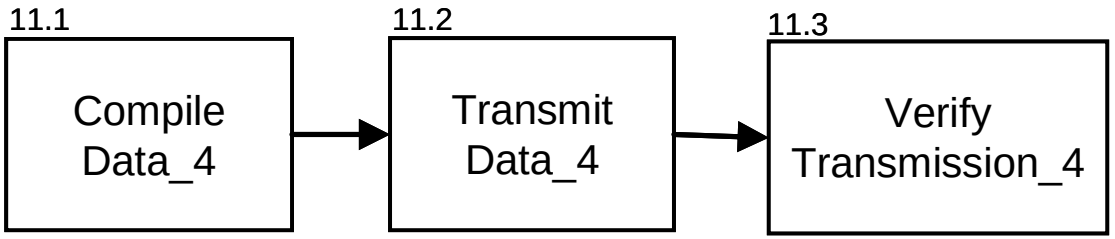

Figure 34. Relay Inventory Information

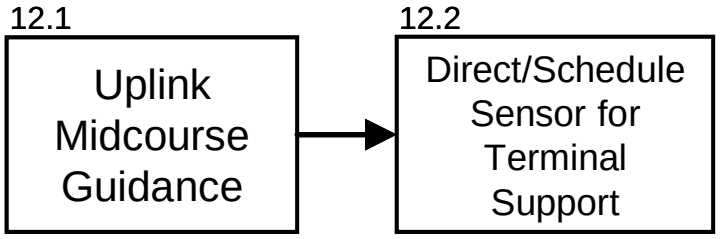

Figure 35. Support Engagement

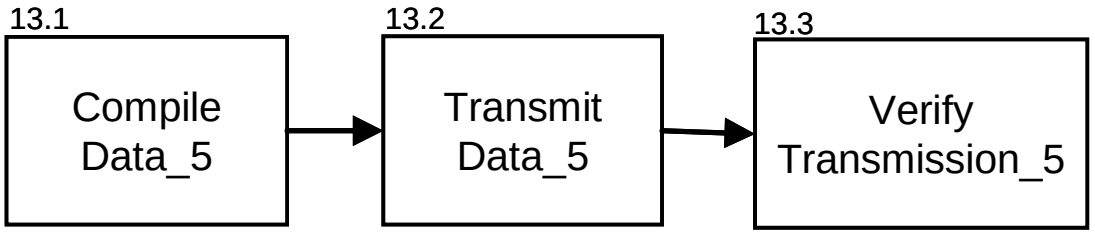

Figure 36. Relay Engagement Data

Conceptual Design Sub-Function FFBDs (Continued)

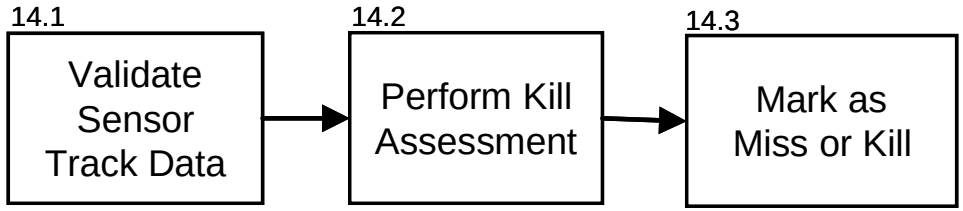

Figure 37. Evaluate Engagement

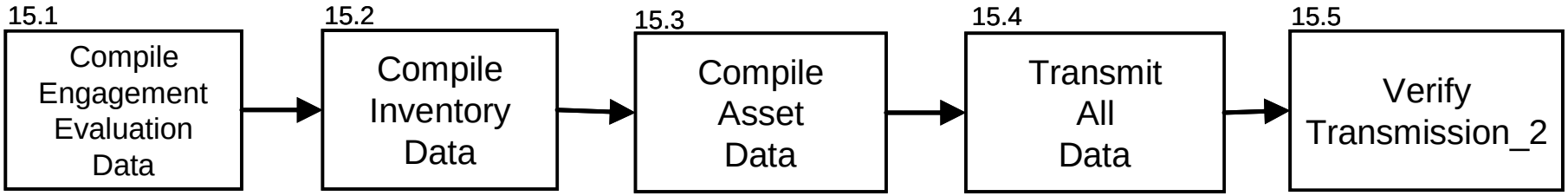

Figure 38. Monitor and Report All Data

2. Modeling

Using a unique methodology, the project provides the following:

1) a characterization of the battle space

2) a description of the design principles applied and

3) a conceptual design.

Computer simulations are used to demonstrate and/or test the functionality of either individual processes within a particular system or the entire system itself. In this project, the functional system architecture was generated utilizing the methods and techniques called out in Blanchard & Fabrycky's systems engineering process (Blanchard-Fabrycky, 2000). A computer-based simulation program (Arena®) was then used to ensure that the overall system was applicable in real-world scenarios. The result was a "system-independent" simulation model containing a representation of each major process within our Open Architecture Domain.

The conceptual design is then modeled using ARENA® simulation software in an attempt to validate the proposed architecture. The FFBDs were used at all three levels as a direct reference for the simulation model. The model simulates data queuing at the platform level as well as at the fire control, tactical, and common operational picture level The simulation model will vary bandwidth and system loading to evaluate data latency concerns, system performance, and data gridlock. The parameters used to setup the model are provided in Appendix B.

The simulation model was developed to represent one CSG or one ESG with call for fire coming in from littoral areas. It was not meant to simulate very large battle space with multiple hubs and points of commend. Figure 38 provides a top-level representation of the Arena® simulation model. The model is comprised of a total of 127 Process Blocks: 14 Top-Level, 53 Secondary, 53 Tertiary, 5 Decide Blocks, 1 Create Block, and 1 Dispose Block. In addition, the model utilizes one return loop to allow for target reengagement in the event that the first interceptor does not defeat the threat. The Tertiary-Level Process Blocks were created to represent the lower level of functions required for the overall functionality of the system. These process blocks are described in

Appendix B. The model utilizes one return loop to allow for target reengagement in the event that the first interceptor does not defeat the threat.

Each of the process blocks utilizes a timing parameter representing the minimum, most likely, and maximum time that the functions occur. In order to prevent the model from becoming classified, only a conservative estimate of each timing parameter was utilized. In the case of this model, adding more process steps increases the amount of conservative error within the steps, thus increasing overall modeling inaccuracy. The model created validates the overall process but does not represent the level of complexity needed to accurately model the system at the component level.

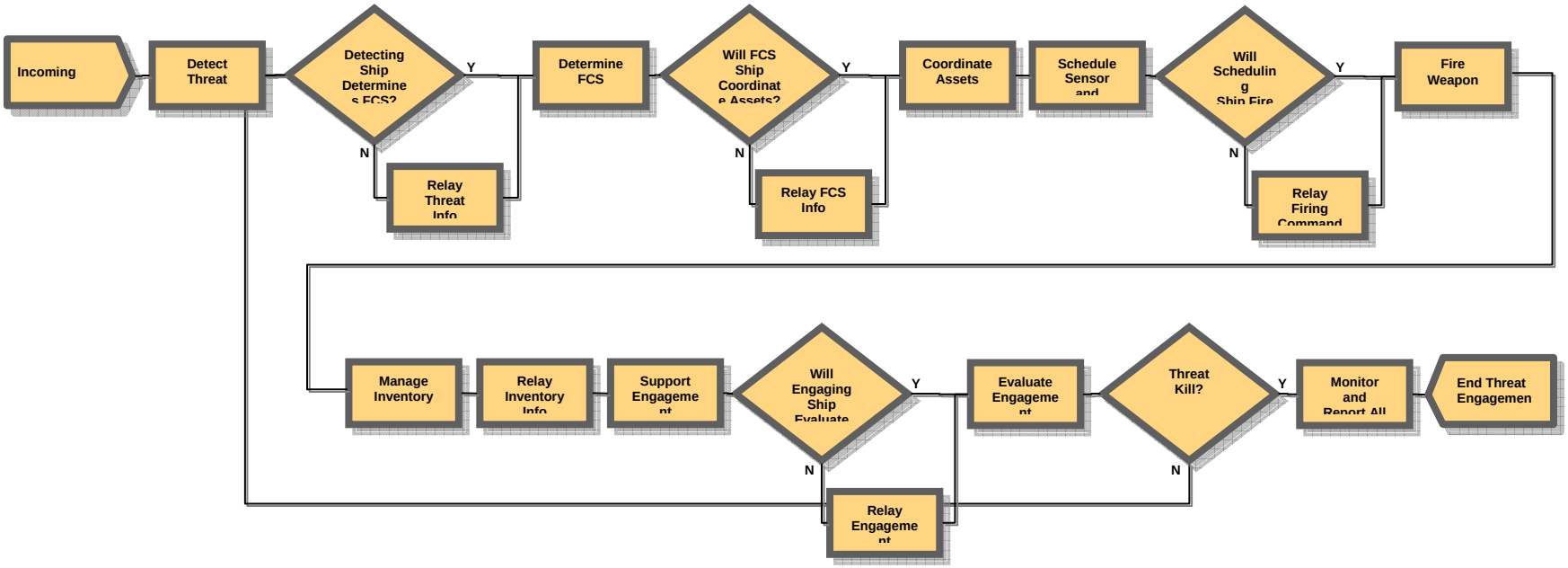

Figure 39. Arena® Simulation Model Layout

IV. RESULTS

A. FORCENET OA DIAGRAMS

The FFBD composition resulted in two high-level FORCEnet OA diagrams that did not differ substantially from the PEO IWS model, used during initial project development. Although the differences are not highly significant, performing the top down, then bottom up decomposition and re-composition provided practical insight to the problem at hand and resulted in a set of conclusions and recommendations. Figure 39 provides a diagram describing the transition between the two models. The text that follows describes the similarities and differences illustrated in Figure 39. The resulting re-composed FORCEnet OA diagrams are then provided in Figures 40 and 41. In order to more clearly explain the results, the model was separated into two diagrams representing both the functional and system domains.

1. **Modeling Technique:** The PEO IWS FORCEnet Model indicates physical groupings of system components in two ways:
    - Functional groupings based on traditional hardware boundaries
    - Notional data flows based on experience with current and legacy systems

    The FORCEnet OA model developed in this project is based primarily on functional flow composition and decomposition. This method of system analysis differs substantially from traditional data flow and hardware boundary based analysis tools and those based on existing commercial Information Technology (IT) systems. This modeling technique allowed the consideration of two diagrams rather than just one during analysis:

    Functional Architecture
    - Sensor management
    - Threat/track management
    - Data fusion/data processing
    - Weapon management

System Domain Architecture

- Prioritized data exchange
- Data inventory and control
- Reporting

This separation allowed for greater detail in developing the OA domain, and allowed insight into potential solutions to the problem of developing FORCEnet OA based on actual implementation of RL, FP and EOR. Language used for levels of information exchange introduced earlier for COP, CTP and FCP will sometimes very between the field activities and their respective contractors. In this project's FORCEnet OA diagrams, the following terms are used interchangeably:

a. G1 – Common Operational Picture

b. G2 – Common Tactical Picture

c. G3 – Fire Control Picture

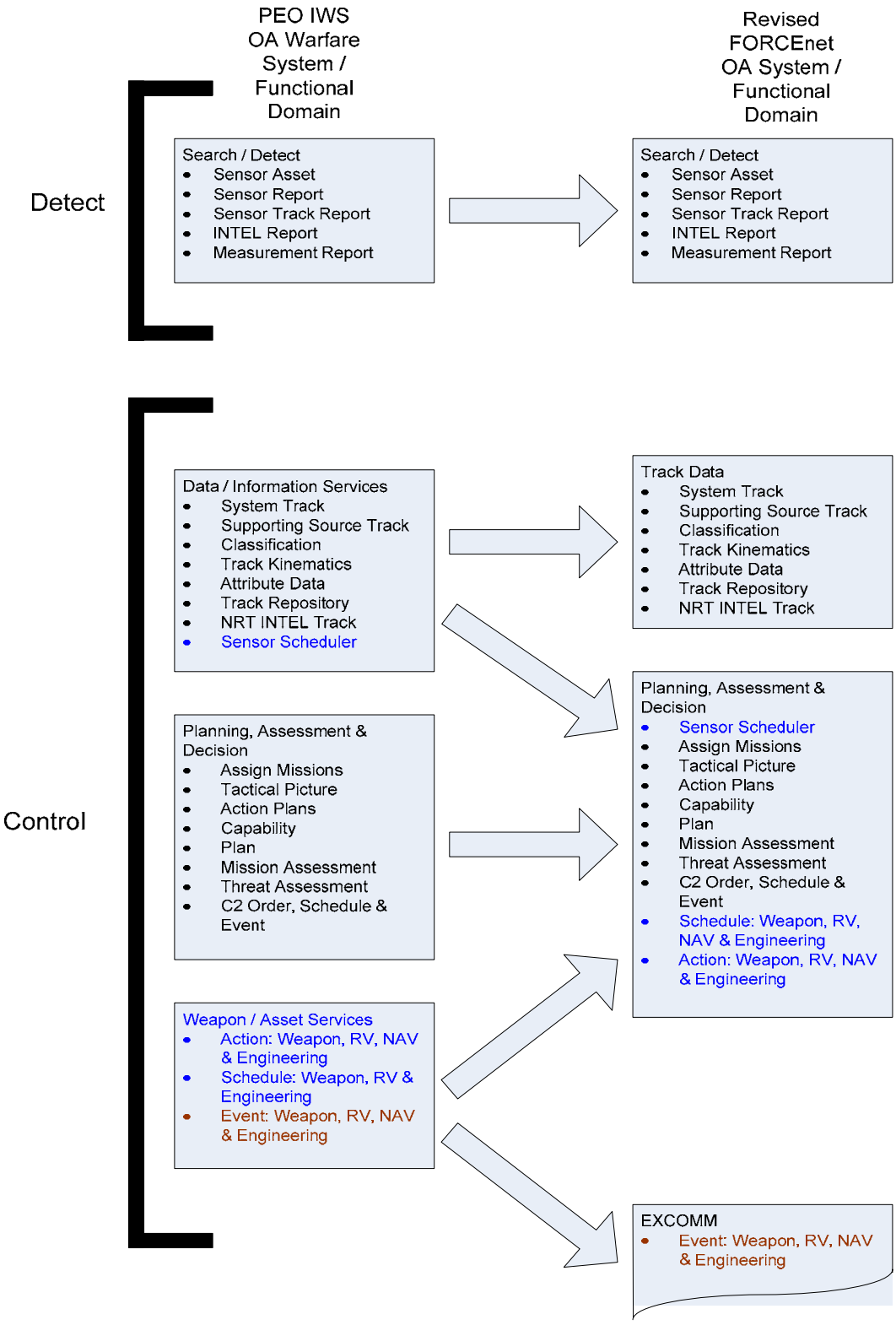

Figure 40. Transition of PEO IWS OA to FORCEnet Model

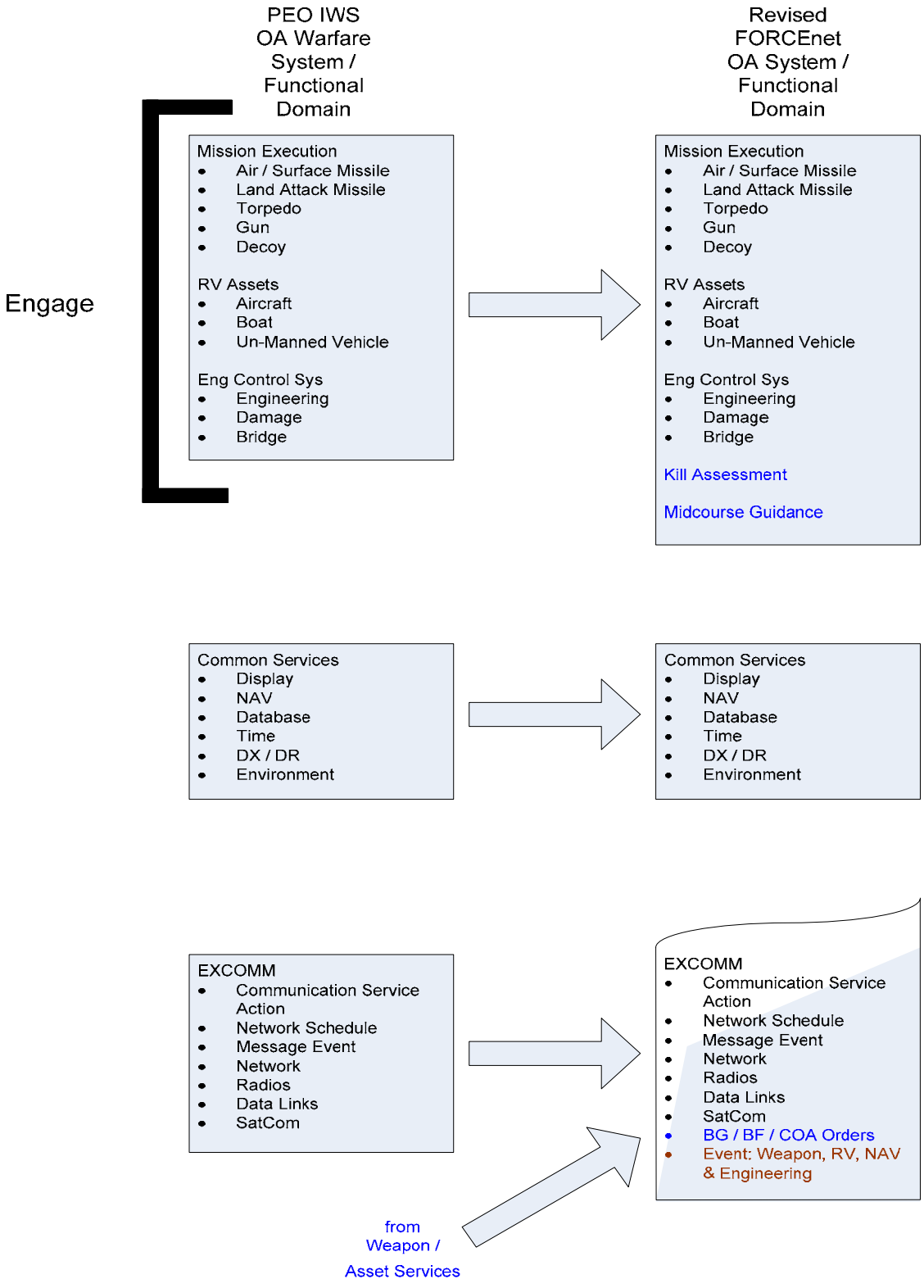

Figure 41. Transition of PEO IWS OA to FORCEnet Model (continued)

2. **PEO IWS FORCEnet Model and FORCEnet OA Model Similarities**: The following functions remained very similar between the two models. The minor differences are noted in the descriptions below. Since the FORCEnet OA model composition created two diagrams rather than one, the primary similarities are most evident comparing the PEO IWS FORCEnet Model to the FORCEnet OA system domain model rather than the functional model. The functional model provides additional detail of what functions are required in each category of the system domain. The following describe the similar functional groupings:

a) **Search and Detect**: This functional block remained almost identical with one exception. The track requires some level of immediate identification so that it can be added to the network for correlation to tracks on other platforms. In order to insure effective reaction time, initial tracks cannot wait for the complete combat identification process before being added to the network.

b) **Data Information Services:** This functional grouping also remained very similar with the following two exceptions:

1) Complete track ID attributes (or full combat ID) was placed within this functional group rather than in Planning, Assessment and Decision. Identification attributes must be assigned sooner within the OODA loop to aid in reaction time.

2) Move the sensor scheduler to planning, assessment and decision where the evolving COP, CTP, and FCP are managed.

c) **Planning, Assessment and Decision**: This functional grouping remained very similar to the PEO IWS model but with the following three added functions:

1) Add sensor scheduler moved from data information services

2) Data fusion opportunity

3) Command and Control and decision-making

d) **Mission Execution**: The primary tasks of this functional block remain the same with some minor tasks added:

1) Inventory Update

2) Midcourse Guidance

3) Kill Assessment

4) Compile and disseminate inventory data

3. PEO IWS FORCEnet Model and FORCEnet OA Model Differences:

As outlined above, the FORCEnet OA system domain model has more in common with the PEO IWS model, while the FORCEnet OA functional model presented major differences. These differences have been categorized and may be described as follows:

a) Weapon Assets and Services Eliminated: This functional category was completely eliminated primarily based on its functions being moved to other functional areas:

1) Action receipt was moved to planning and assessment in order to increase reaction time. The system will immediately take action on assigned missions.

2) Scheduling was moved to planning and assessment in order to make a decision and immediately schedule and add status to the network. This incorporates sensors input as part of an overall planning, assessment and decision-making. It also eliminates the possible network data traffic congestion since processing power requirement is no longer an issue (dual cores, quad cores, etc.).

3) Event was moved to EXCOMM in order to update the COP and CTP in parallel with taking action in mission execution

b) **Force Planning and Coordination Eliminated**: Joint Battle Force Orders (JBFO) and Battle Group Orders (BGO) will be broadcast to all platforms simultaneously. The orders will be processed through common services and received via EXCOMM. Each platform will use this information dependent on their view and involvement in the battle space.

c) **EXCOMM Considerably Expanded** – EXCOMM has the same system domain physical hardware function as the original PEO IWS model. It remains manager of networks, radio, and satellite communications. These functions are managed so that, based on the best data rate that the system is actually experiencing, there is reasonable data flow to the CTP and COP. Without monitoring and managing data flow, and choosing alternative network paths or communication vehicles, data flow disruptions could potentially cripple the system. Although initial dominance of the battle space may be achieved, maintenance of that domination may be suspect based on network problems, gridlock, or singular data paths. The role of EXCOMM, therefore, has expanded to assume the "event status" of weapon/asset services and integrates more directly with common services. EXCOMM will call on various communication paths dependent on data priority and security requirements for FCS transmission, track/threat updates, and direct receipt of intelligence data. The FCP, CTP and COP are constantly evolving, and FORCEnet must react in both a time constrained manner, dependent on threat priority, and in a command and control manner to update the CTP and COP based on updates from kill assessments, data fusion, sensor reassignment, and platforms joining and exiting the battle space. EXCOMM must also coordinate with other system functions to update data tags such as timing, type, and track quality prior to transmission or adding this data to the network. Working with common services, EXCOMM will need to compensate for network loading, choose alternate data paths based on data priority and FCP urgency. Networks will slow or

crash, and EXCOMM, in conjunction with common services, will be required to not only manage down times and alternative paths, but anticipate slowing data rates due to system loading and react.

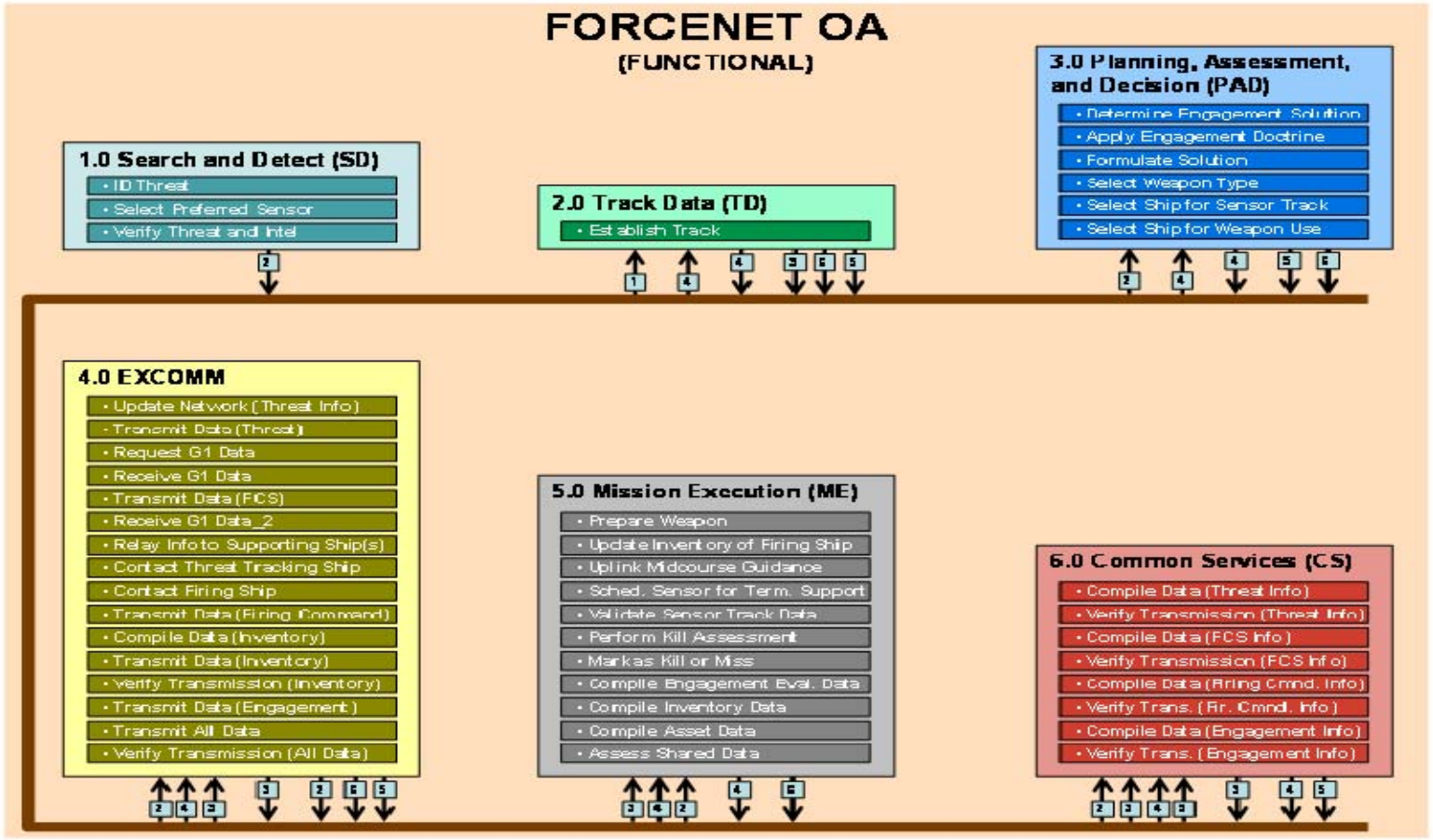

Figure 42. Revised Functional FORCEnet OA Model

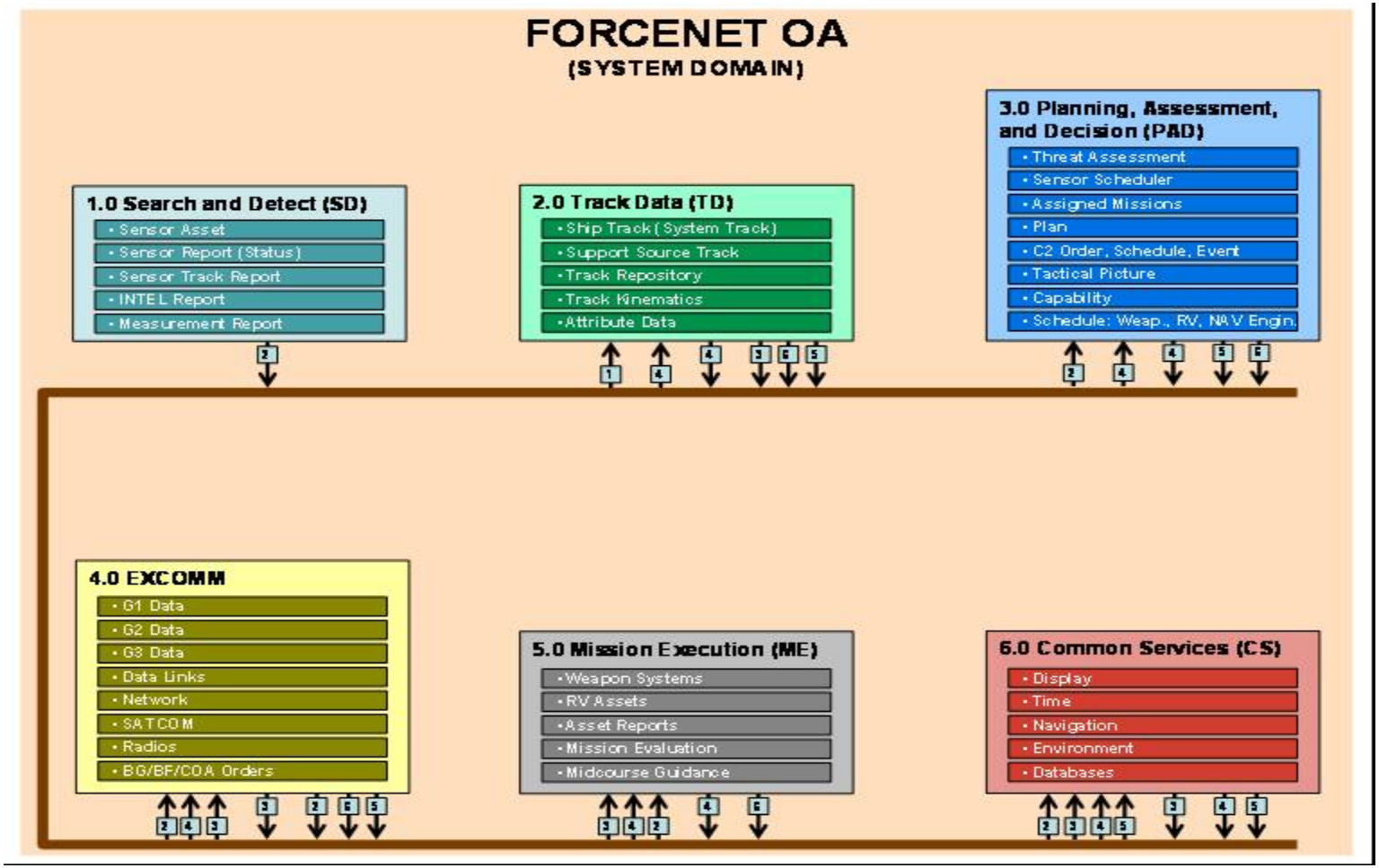

Figure 43. Revised FORCEnet OA System Domain Model

B. SIMULATION MODEL RESULTS

The Arena model was run based on data packet assignments provided in Table 1.

Data Packet	Transfer Type	Transmitted Data	Process Step	Operational Context
G1.1	Peer-to-Peer	Threat Track Info	Relay Threat Info	FCP
G1.2	Peer-to-Peer	FCS	Relay FCS Info	FCP
G1.3	Peer-to-Peer	Schedule Info	Schedule Sensor/Weapon	FCP
G1.4	Peer-to-Peer	Firing Commands	Relay FCS Info	FCP
G1.5	Peer-to-Peer	Inventory Data	Relay Inventory Info	FCP/CTP
G1.6	Peer-to-Peer	Engagement Data	Relay Inventory Info	FCP
G2.1	Broadcast	Inventory Data	Relay Inventory Info	CTP
G3.1	Broadcast	All Data	Monitor and Report All Data	COP

Table 1. **Data Packet Assignments**

Table 2 below displays the results collected from the ARENA model using the individual process timing parameters provided in the Appendix. The total number of incoming threats, the interval between each set of incoming threats, and the percentage of successful initial engagements was varied for each of the eight model runs. For each model run, a total of 100 replications were carried out with a maximum of 10 threat arrivals.

# of Incoming Threats	Threat Interval (seconds)	% of Successful First-time Engagements	WIP [Saturation] (seconds)	Average Total Time (seconds)	Limiting Process #1	Limiting Process #1 Time (seconds)	Limiting Process #2	Limiting Process #2 Time (seconds)
1	60	90	0.5166	25.1135	"ID the Threat"	0.3694	"Establish a Track"	0.2561
1	60	100	0.4974	23.4344	"ID the Threat"	0.3551	"Establish a Track"	0.2648
1	30	90	1.2893	34.8877	"ID the Threat"	0.872	"Determine an Engagement Solution"	0.5203
1	30	100	1.2033	32.1173	"ID the Threat"	0.8961	"Establish a Track"	0.4846
2	60	90	2.3242	63.4865	"Transmit All Data"	2.0821	"Compile Inventory Data"	1.7562
2	60	100	2.2656	59.8616	"Transmit All Data"	2.3936	"Compile Inventory Data"	1.9017
2	30	90	5.8229	120.15	"Transmit All Data"	3.3926	"Compile Inventory Data"	3.0117
2	30	100	5.7013	111.14	"Transmit All Data"	3.7807	"Compile Inventory Data"	3.271

Table 2. **Run Results**

Based on the results outlined in Table 2, the following observations were made:

- As the number of incoming threats was increased from 1 to 2, the average total system time more than doubles while the system saturation increases four-fold.
- Going from 30 to 60 second long threat interval time increases both the average total system time and system saturation by 2.5 times.
- Reengaging 10% of the time means about a 5-10% increase in average total system time with a slight increase in system saturation.
- Key drivers of system saturation are 1) number of incoming threats and 2) threat interval.

Limiting factor tends to vary. For a single incoming threat, “ID the Threat” is the primary driver while “Establish a Track” is the secondary driver. For two incoming threats, "Transmit All Data" is the primary driver while "Compile Inventory Data" is the secondary driver. In both cases, the OA communication tends to get saturated but not the actual threat engagement.

Using this computer-based simulation model, the following two results were considered significant:

1. **Validation of the model structure**. The model verified that the proposed system possessed a logical flow with no apparent lapses while addressing the functionality requirements for each of the three threat engagement scenarios. The lowest level process blocks within the model form a chain of components that resemble a logical flow. This portion of the model demonstrates an adequate level of functionality with no unnecessary redundancy or unrealistic steps.

2. **Validation of system timing.** The model was modified so that each of the various sub-models closely represented actual ship system elements whenever possible. This was accomplished by defining both a specific system resource and its associated timing parameters within each of the lowest level process modules. With the use of timing parameters, it was determined that there were no excessive

bottlenecks within the proposed system. A more accurate representation may be created through the use of actual shipboard timing parameters. This model could then be used in simulation testing, statistical analysis, and for future process improvements (e.g., Lean, six sigma, and theory of constraints).

Additional benefits may come from the use of an advanced computer-based simulation application, one that includes the ability to readily display a tactical representation of the integrated systems in a simulated operational environment. During simulation events many scenarios may be run and large amounts of data extracted in order to attain a high confidence level of systems performance prior to finalized design.

V. CONCLUSIONS AND RECOMMENDATIONS

The analysis performed for this research project has exposed potential functional boundary limitations in the currently proposed PEO IWS OA Functional Domain model as presented, and a revised OA Functional Domain model has been offered for consideration. Through simulation development, test execution and the use of systems engineering techniques, this re-structured model has been evaluated and appears to satisfy OA and FORCEnet requirements for the specific Mission Capability Packages examined. This model and its simulation component do bear further scrutiny and refinement to ensure the processes and their attributes are properly characterized. The recommendation is for this review to be performed by Engagement or FORCEnet Subject Matter Experts (SMEs) who could provide constructive feedback regarding the level of accuracy and realism contained therein. Additional benefits may be gained from expanding the Simulation model to increase the number of FORCEnet platform participants so as to determine the point at which the OA model becomes inefficient and/or ineffective. OA specifications and system boundary descriptions will eventually attain capacity levels with respect to data flow. This point of diminishing return relative to battle space size should be identified, realized, and modeled. It is the hope and expectation that the work performed in support of this thesis may be partially or fully adopted by future research projects to further develop, test and validate the feasibility of additional FORCEnet mission requirements operating within the Open Architecture functional construct.

Research efforts have demonstrated that across the Navy Enterprise, FORCEnet viability, affordability, and sustenance necessitates an architecture that is in full compliance with Open Architecture technology, systems and standards. The continued presence of legacy and non-OA computer and operational systems within the FORCEnet construct will only prevent FORCEnet-wide Combat System enhancements from being beneficial to all force-level participants. Service-specific acquisition projects will continue to limit and constrain efforts to enable Joint Coordination and establish effective Battle Space management in support of the Navy's Sea-Power 21 and Single Integrated Air Picture initiatives. To successfully combat the more challenging threats of the 21st

century, current and future warfighting capabilities demand a full adoption of OA standards and infrastructure. We believe that the OA functional assessment and model validation provided herein gives credence to the belief that the development and embedding of Open Architecture within FORCEnet will result in a superior, adaptive, "plug and fight" capability for the modern war-fighter of today and tomorrow.

APPENDIX A. INTEGRATED ARCHITECTURE PRODUCTS

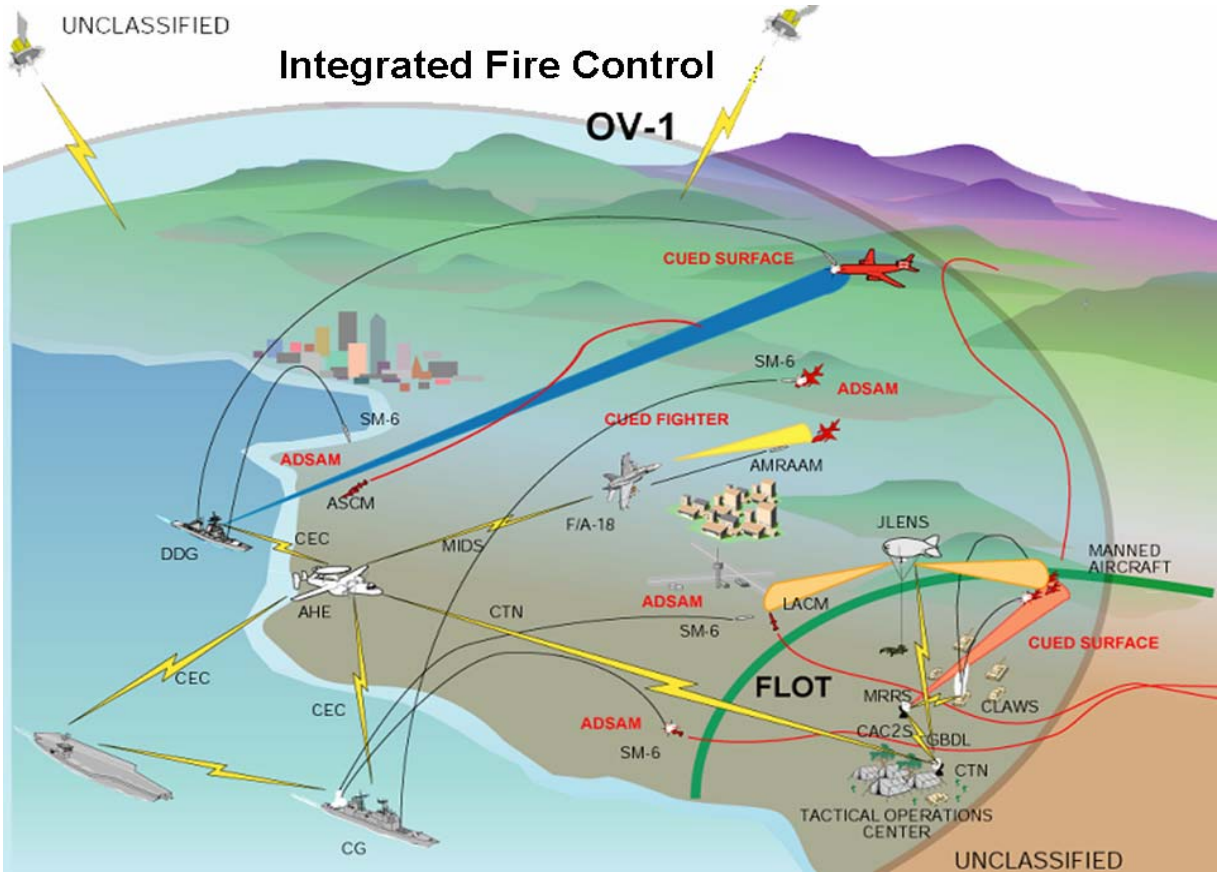

Figure A-1: OV-1 IFC Scenario Operational Concept (PEO IWS, 2006)

The Integrated Fire Control (IFC) High Level Operational Concept (OV-1) provides a high-level illustration of the mission, highlighting the main operational nodes involved and the unique operational aspects of intended environment. The OV-1 is a pictorial representation of the expected interactions between the systems and their environment. Its primary purpose is to facilitate communications between the warfighters and produce then execute a successful Integrated Fire Control Solution.

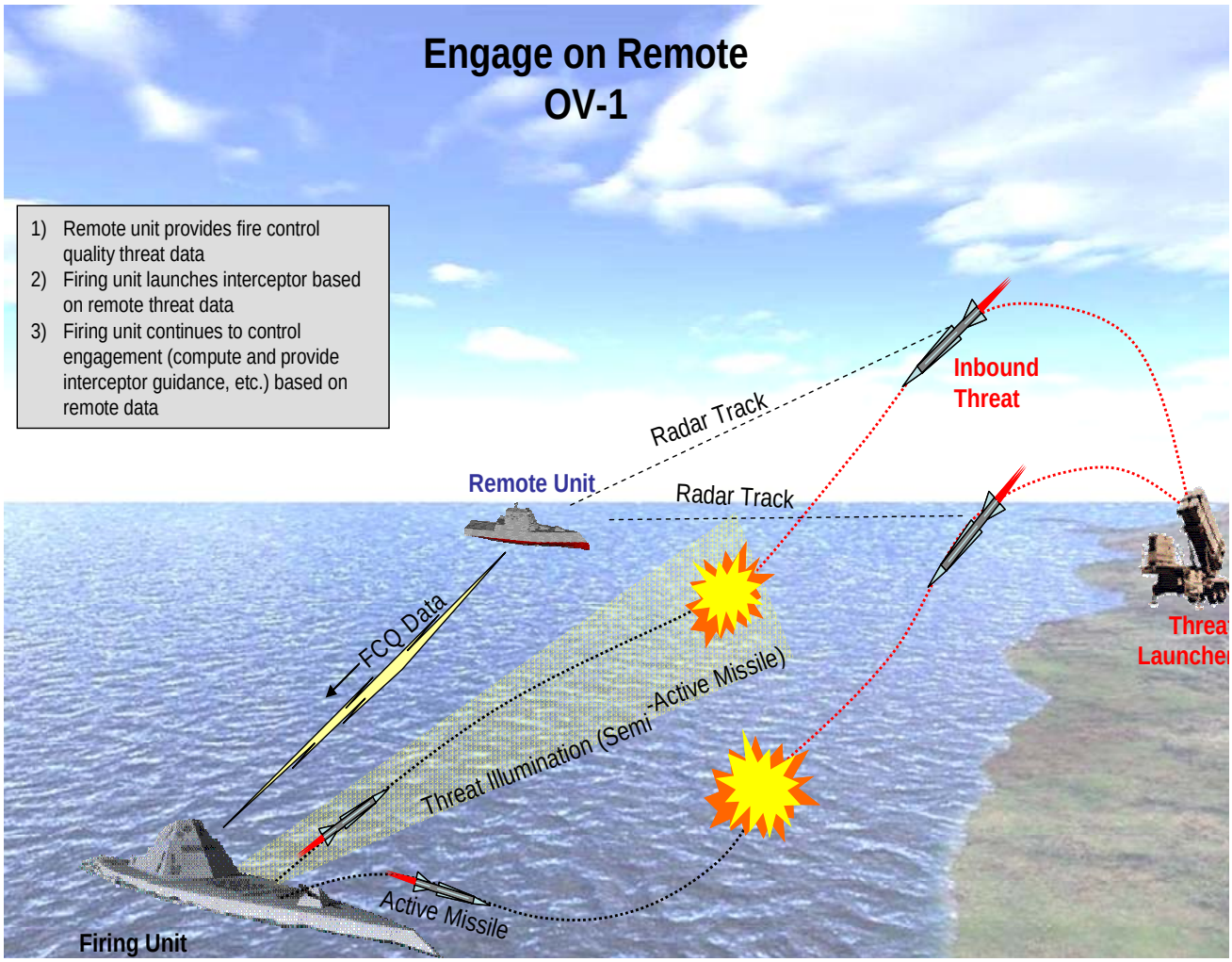

Figure A-2: OV-1 Engage on Remote Scenario Operational Concept

The purpose of the OV-1 Engaged on Remote (EOR) diagram is to depict the engagement of a threat where a remote unit provides the Fire Control Quality threat data to the Firing Unit platform. Using this remote data, the Firing Unit launches an interceptor at the threat, while the remote unit continues to direct and control engagement.

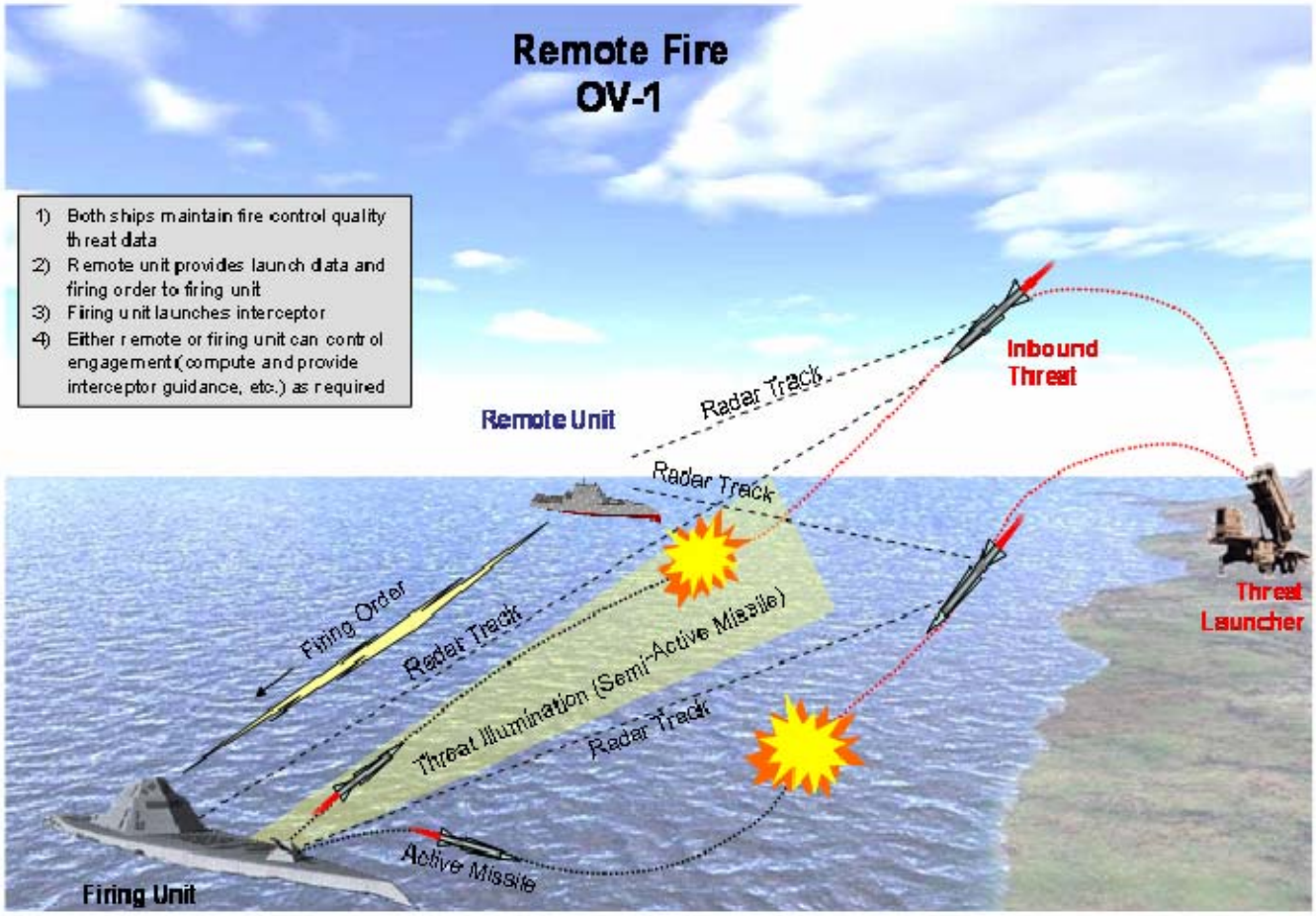

Figure A-3: OV-1 Remote Fire Scenario Operational Concept

The purpose of the OV-1 Forward Pass diagram is to provide a graphical representation of a scenario where the control of an in-flight missile is handed off to another equally capable unit to complete the intercept. The Firing Unit launches interceptor then transfers the remainder of engagement prosecution to remote unit. Essentially, the Remote Unit takes over an in-process engagement initiated by another Unit.

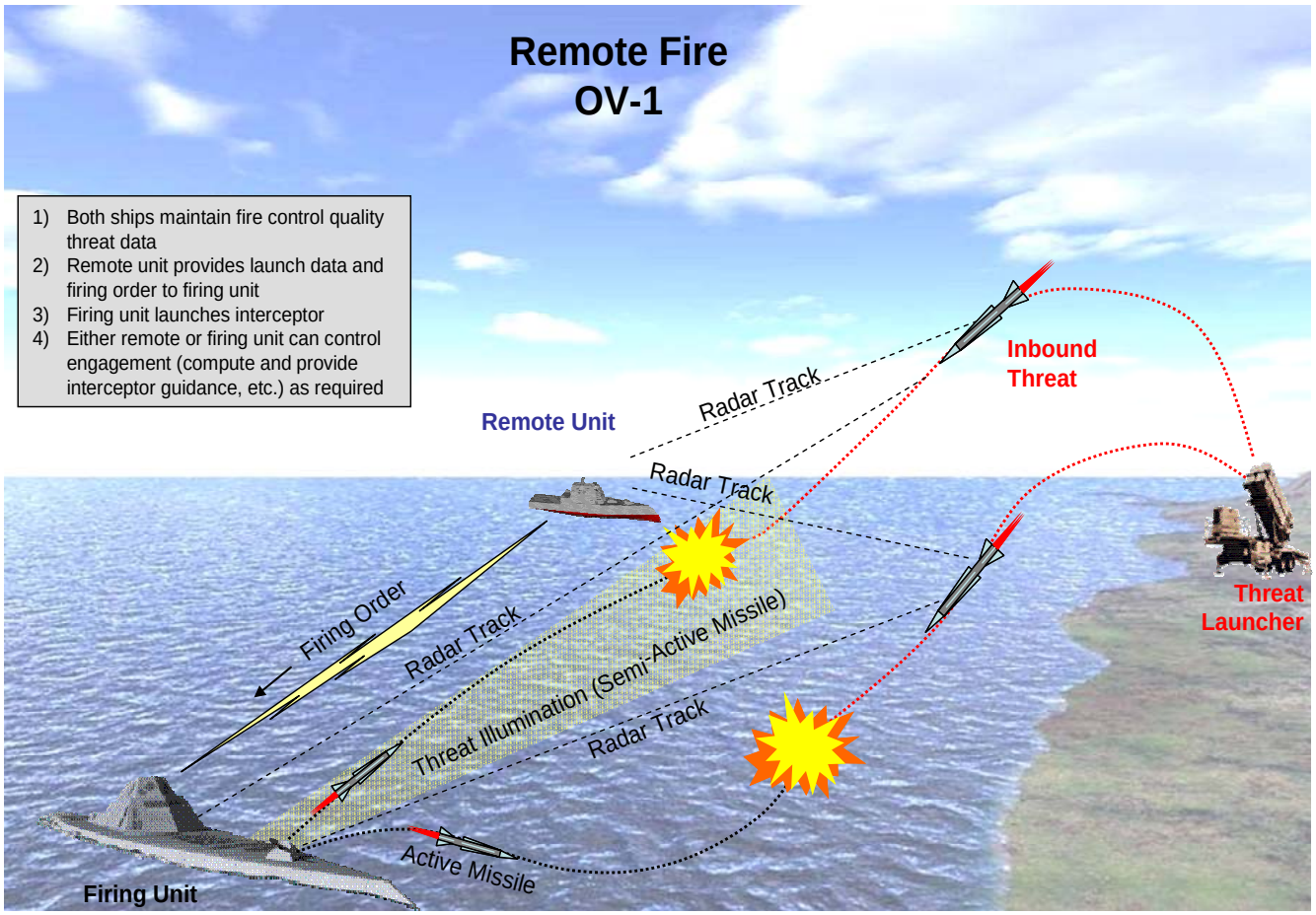

Figure A-4: OV-1 Remote Fire Scenario Operational Concept

The purpose of the OV-1 Remote Fire diagram is to provide a graphical representation of a scenario where the control of an in-flight missile is handled by another equally capable unit to complete the intercept. The Firing Unit provides launch of the interceptor only. Essentially, the Remote Unit launches the weapon, but the local unit provides the FCS and supports the interceptor in-flight. If the interceptor has its own on-board illuminator, it may fly autonomously to the target.

EOR OPERATIONAL SCENARIOS AND SEQUENCE DIAGRAMS

The remote unit will sense threat information and transfer it to the firing unit. The remote unit will transmit a firing request to the firing unit. The firing unit will then use the remote threat data to launch an interceptor. The remote unit will continue to control the engagement based on the remote unit data.

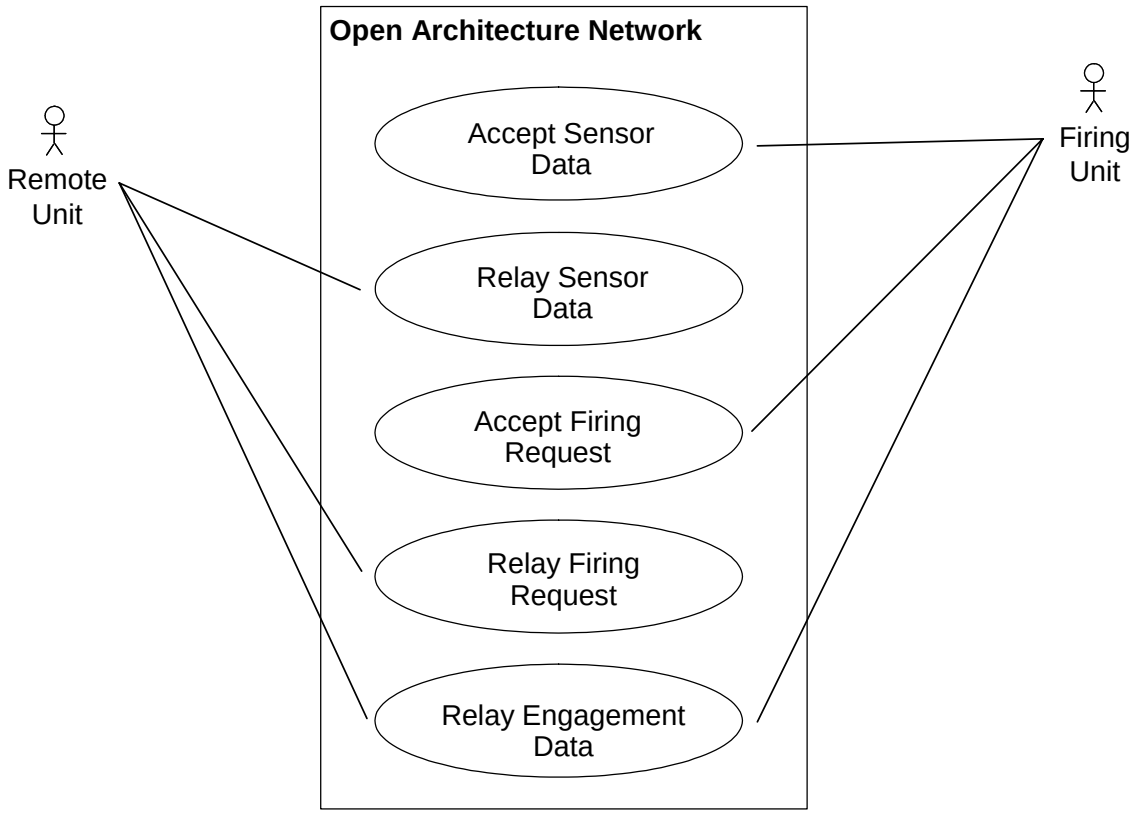

Figure A-5: Engage on Remote Use Case Diagram

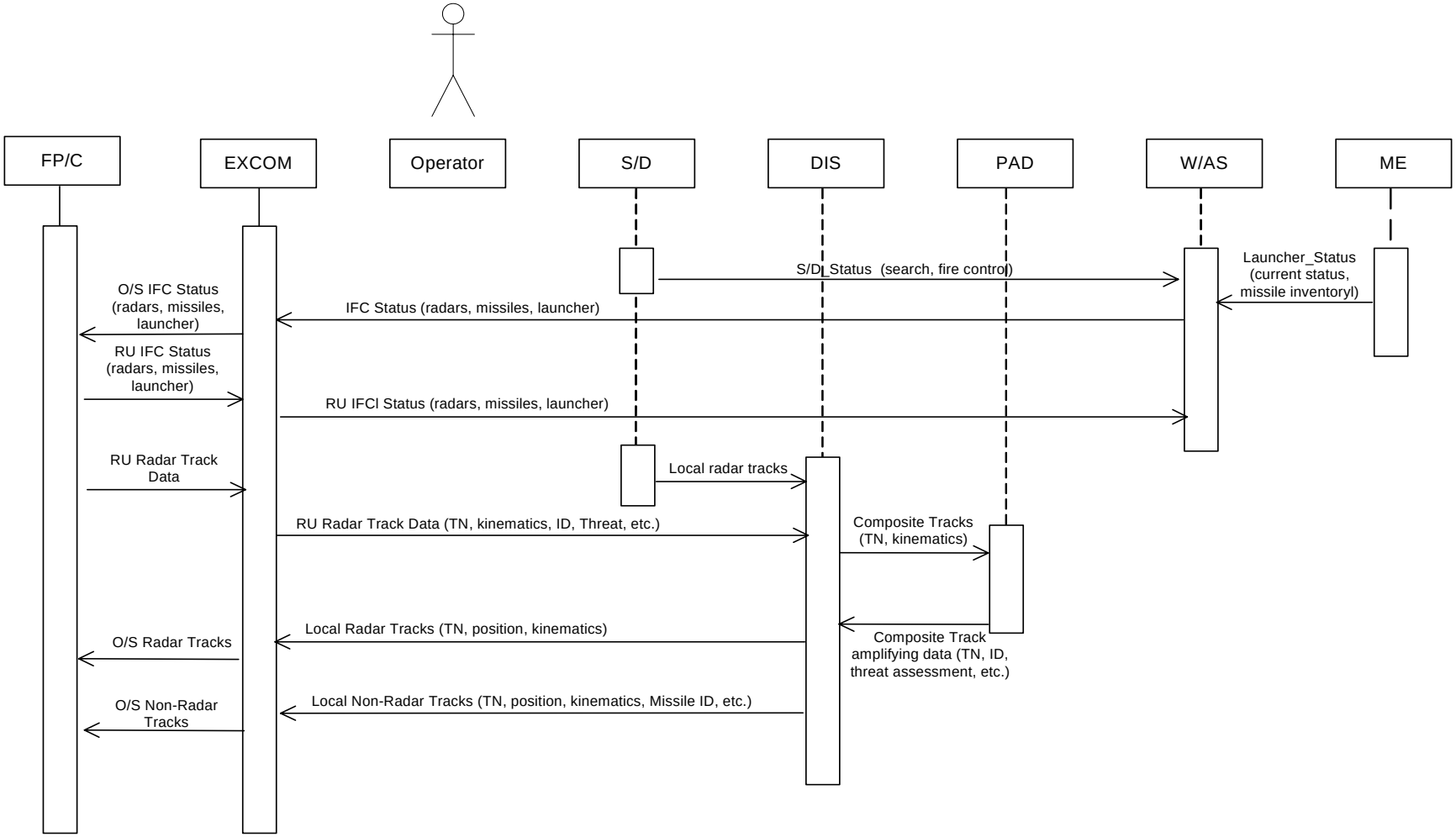

Figure A-6: EOR Operational Sequence Diagram #1

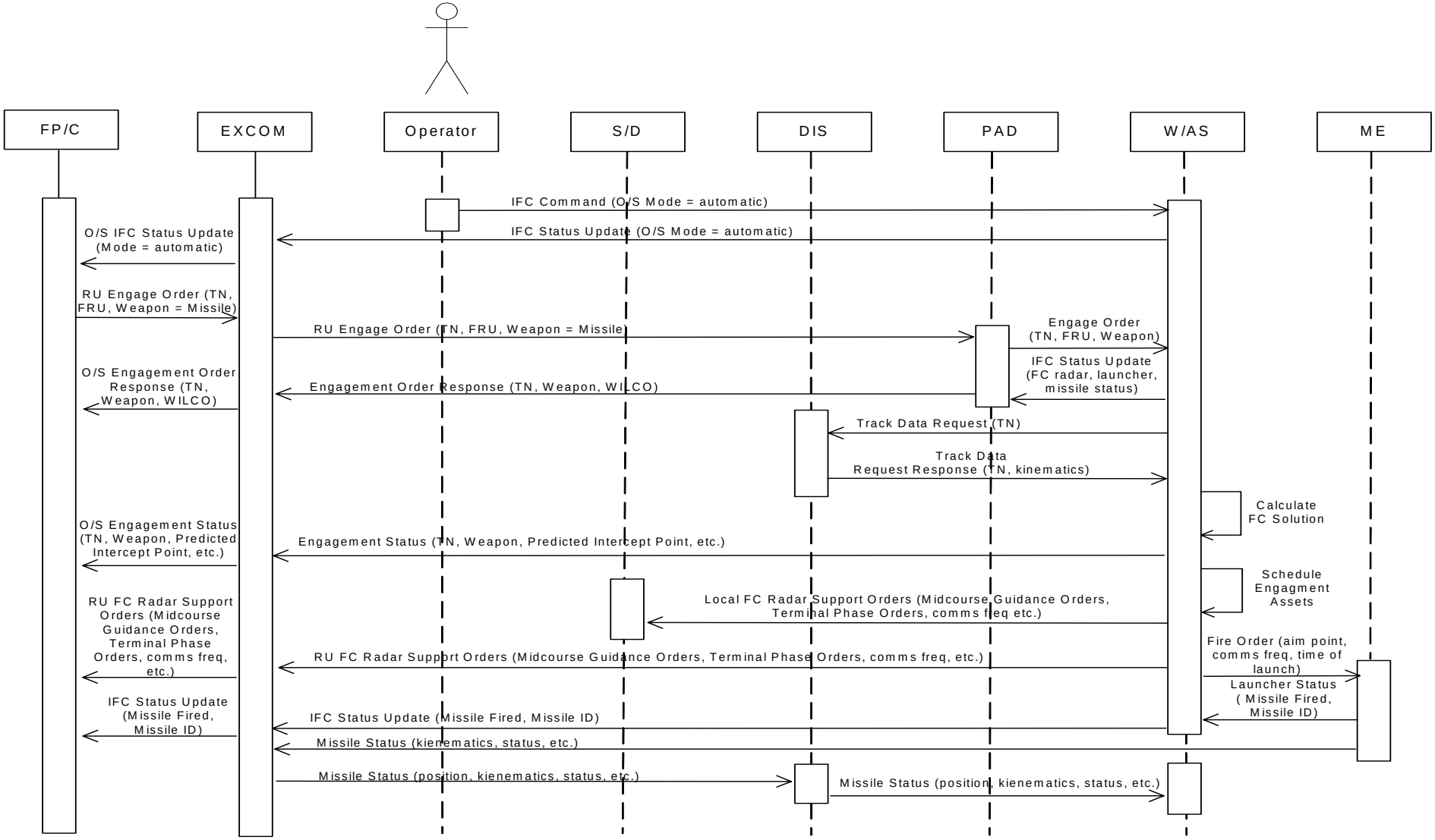

Figure A-7: EOR Operational Sequence Diagram #2

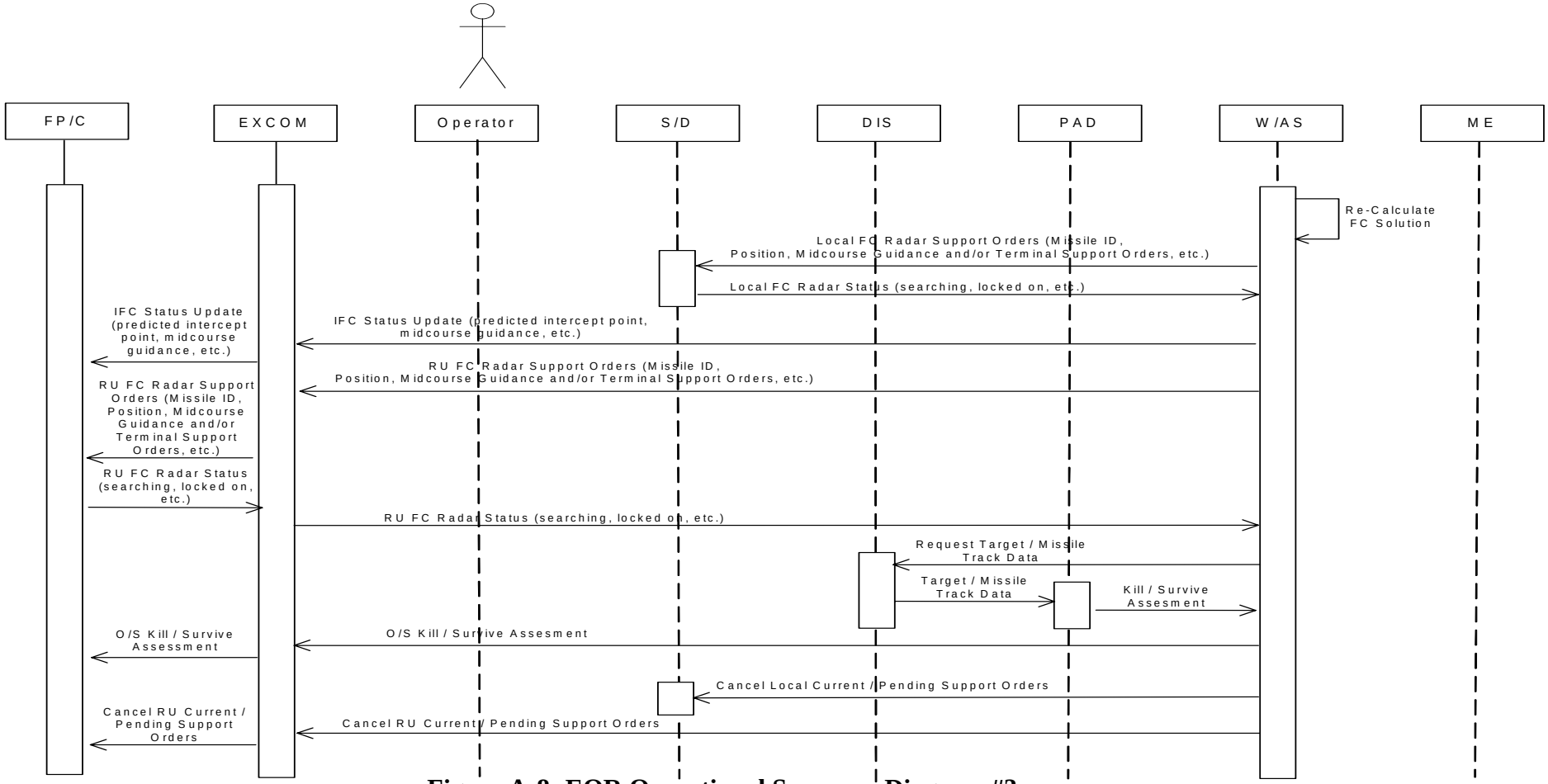

Figure A-8: EOR Operational Sequence Diagram #3

APPENDIX B. ARENA® SIMULATION MODEL

Appendix B is divided into two parts, section A-1 describes each of the process blocks within the model, and section A-2 describes the parameters used to develop the model in a spreadsheet.

A-1 ARENA MODEL PROCESS BLOCK DESCRIPTIONS

I) **Incoming Threat –** Represents the threats entering the Naval Battle Group operational area. This includes threats entering into the individual operational area of any one ship within the Battle Group as well as the overall operational area established by the Battle Group Commander.

II) **Detect Threat –** Top-level sub-model containing lower-level processes which represent a ship's ability to manage incoming threats. The lower-level processes contained within this sub-model are as follows:

a. ID Threat – Threat is identified as entering into a ship's operational area.
b. Select Preferred Sensor – Ship allocates a preferred sensor to handle the tracking duties for the particular threat(s).
c. Establish Track – A solid track of the threat is established.
d. Verify Threat and Intel – Using pre-gathered intelligence information, the ship verifies whether the threat is actually a known threat or if the threat is actually a friendly force.
e. Update Network – The ship updates the network with information regarding the threat.
f. Determine Engagement Solution – The ship determines how to proceed in engaging the threat.

III) **Will Detecting Ship Determine FCS? –** Decision block determining whether the ship which detected the threat will 1) determine the Fire Control Solution

(FCS) for engaging the threat or 2) pass along the duty of determining the FCS to another ship. If the ship which detected the threat will determine the FCS, the next step will be to proceed to "Determine FCS." If the duty of determining the FCS is to be passed to another ship, the next step will be to proceed to "Relay Threat Info."

IV) **Relay Threat Info –** Top-level sub-model containing lower-level processes which represent the act of a ship in relaying track data of a threat to another ship. The lower-level processes contained within this sub-model are as follows:

a. Compile Data – The threat track data is gathered into an electronic packet of information suitable for transmission.
b. Transmit Data – Electronic packet of threat track data is transmitted to another ship.
c. Verify Transmission – The transmitting ship verifies that the information packet was received by the other ship.

V) **Determine FCS –** Top-level sub-model containing lower-level processes which represent the act of a ship in determining the proper FCS for engaging the threat. The lower-level processes contained within this sub-model are as follows:

a. Request G1 Data – Ship determining the FCS requests all known threat data from the G1 high-speed data line.
b. Gather G1 Data – Ship determining the FCS gathers the threat data received from the G1 high-speed data line.
c. Apply Engagement Doctrine – Ship compares parameters of threat to pre-set ship engagement doctrine.
d. Formulate Solution – Ship formulates a solution based on the results specified in the ship engagement doctrine.

VI) **Will FCS Ship Coordinate Assets? –** Decision block determining whether the ship which determined the FCS will 1) coordinate the assets necessary for engaging the threat or 2) pass along the duty of coordinate the assets necessary for engaging the threat to another ship. If the ship which determined the FCS will coordinate the assets necessary for engaging the threat, the next step will be to proceed to "Coordinate Assets." If the duty of coordinate the assets necessary for engaging the threat is to be passed to another ship, the next step will be to proceed to "Relay FCS Info."

VII) **Relay FCS Info –** Top-level sub-model containing lower-level processes which represent the act of a ship in relaying FCS info to another ship. The lower-level processes contained within this sub-model are as followed:

a. Compile Data – The FCS info is gathered into an electronic packet of information suitable for transmission.
b. Transmit Data – Electronic packet of FCS info is transmitted to another ship.
c. Verify Transmission – The transmitting ship verifies that the information packet was received by the other ship.

VIII) **Coordinate Assets –** Top-level sub-model containing lower-level processes which represent the act of a ship in coordinating the assets necessary for engaging the threat. The lower-level processes contained within this sub-model are as followed:

a. Gather G1 Data – Ship responsible for coordinating the assets necessary for engaging the threat gathers all known threat data from the G1 high-speed data line.
b. Select Weapon Type – The appropriate weapon type is selected based on the Engagement Doctrine.
c. Select Ship for Sensor Track – Ship is selected to perform sensor track role.

d. Select Ship for Weapon Use – A ship which can provide the necessary intercept weapon is selected.
e. Relay Info to Supporting Ship – If a supporting ship was established, then asset info is relayed to that ship.

IX) **Schedule Sensor and/or Weapon –** Top-level sub-model containing lower-level processes which represent the act of a ship in scheduling a sensor and/or weapon necessary for engaging the threat. The lower-level processes contained within this sub-model are as follows:

a. Contact Threat Tracking Ship – The ship responsible for tracking the threat is contacted.
b. Contact Firing Ship – The ship responsible for firing the asset is contacted.
c. Prepare Weapon – The intercept weapon is initially prepared for launch.

X) **Will Scheduling Ship Fire Weapon? –** Decision block determining whether the ship which scheduled the sensor and/or weapon necessary for engaging the threat will 1) fire the intercept weapon or 2) pass along the duty of firing the intercept weapon to another ship. If the ship which scheduled the sensor and/or weapon necessary for engaging the threat will fire the intercept weapon, the next step will be to proceed to "Fire Weapon." If the duty of firing the intercept weapon is to be passed to another ship, the next step will be to proceed to "Relay Firing Command Info."

XI) **Relay Firing Command Info –** Top-level sub-model containing lower-level processes which represent the act of a ship in relaying the firing command info to another ship. The lower-level processes contained within this sub-model are as follows:

a. Compile Data – The firing command info is gathered into an electronic packet of information suitable for transmission.

b. Transmit Data – Electronic packet of the firing command info is transmitted to another ship.
c. Verify Transmission – The transmitting ship verifies that the information packet was received by the other ship.

XII) **Fire Weapon –** Top-level sub-model containing lower-level processes which represent the act of a ship in firing the intercept weapon responsible for engaging the threat. The lower-level processes contained within this sub-model are as followed:

a. Provide Shipboard Power to Weapon – Ship responsible for firing the weapon provides shipboard power to the intercept asset.
b. Provide Initialization Data to Weapon – Ship responsible for firing the weapon provides initialization power to the intercept asset.
c. Activate Weapon Batteries – Ship responsible for firing the weapon removes shipboard power after providing the necessary command to activate the weapon batteries.
d. Provide INTENT TO LAUNCH Command – Ship responsible for firing the weapon provides the final launch command necessary for release of the intercept asset.
e. Assign Launch Status – A launch status is assigned to the intercept asset which marks it as a successful or unsuccessful weapon launch.
f. Provide Weapon Status – Ship responsible for firing the weapon provides the weapon status (i.e. launch status).

XIII) **Manage Inventory –** Top-level sub-model containing lower-level processes which represent the act of a ship in managing its weapon inventory. The lower-level processes contained within this sub-model are as follows:

a. Update Inventory of Firing Ship – The weapon inventory for the magazine of the firing ship is updated to reflect any changes (i.e. recent launches/misfires/duds).

b. Compile Data – The updated weapon inventory data is gathered into an electronic packet of information suitable for transmission.
c. Transmit Data – Electronic packet of updated weapon inventory data is transmitted electronically to ship command and control.
d. Verify Transmission – The ship verifies that the information packet was received within command and control.

XIV) **Relay Inventory Info –** Top-level sub-model containing lower-level processes which represent the act of a ship in relaying its updated inventory info to all other ships. The lower-level processes contained within this sub-model are as follows:

a. Compile Data – The updated weapon inventory data is gathered into an electronic packet of information suitable for transmission.
b. Transmit Data – Electronic packet of updated weapon inventory data is transmitted to the other ships within the battle group.
c. Verify Transmission – The transmitting ship verifies that the information packet was received by the other ships within the battle group.

XV) **Support Engagement –** Top-level sub-model containing lower-level processes which represent the act of a ship in supporting the engagement of a threat by an intercept weapon. The lower-level processes contained within this sub-model are as follows:

a. Uplink Midcourse Guidance – The ship responsible for supporting the threat engagement uplinks to the intercept weapon and provides all necessary midcourse guidance commands.
b. Direct/Schedule Sensor for Terminal Support – The ship responsible for supporting the threat engagement directs or schedules a sensor and illuminator to provide terminal support to the intercept weapon.

XVI) **Will Engaging Ship Evaluate the Engagement? –** Decision block determining whether the ship responsible for engaging the threat will 1) evaluate the engagement or 2) pass along the duty of evaluating the engagement to another ship. If the ship responsible for engaging the threat will evaluate the engagement, the next step will be to proceed to "Evaluate Engagement." If the ship responsible for engaging the threat will pass along the duty of evaluating the engagement to another ship, the next step will be to proceed to "Relay Engagement Data."

XVII) **Relay Engagement Data –** Top-level sub-model containing lower-level processes which represent the act of a ship in relaying engagement data to all other ships. The lower-level processes contained within this sub-model are as follows:

a. Compile Data – The engagement data is gathered into an electronic packet of information suitable for transmission.
b. Transmit Data – Electronic packet of engagement data is transmitted to the other ships within the battle group.
c. Verify Transmission – The transmitting ship verifies that the information packet was received by the other ships within the battle group.

XVIII) **Evaluate Engagement –** Top-level sub-model containing lower-level processes which represent the act of a ship in evaluating the engagement of a threat by an intercept weapon. The lower-level processes contained within this sub-model are as follows:

a. Validate Sensor Track Data – The sensor track data collected during the engagement of the threat is analyzed and validated.
b. Perform Kill Assessment – A kill assessment is performed to determine if both the threat and the intercept weapon were destroyed.
c. Mark as Miss of Kill – The engagement is scored as either a hit or miss.

XIX) **Threat Kill? –** Decision block determining whether the threat was destroyed or not. If the threat was destroyed, the next step will be to proceed to "Monitor and Report All Data." If the threat was not destroyed, the next step will be to proceed back to "Will Detecting Ship Determine FCS" to allow for a possible reengagement with another intercept weapon.

XX) **Monitor and Report All Data –** Top-level sub-model containing lower-level processes which represent the act of a ship in monitoring and reporting all data from a previous threat engagement activity to all other ships. The lower-level processes contained within this sub-model are as follows:

a. Compile Engagement Evaluation Data – Engagement evaluation data is gathered into an electronic packet of information suitable for transmission.
b. Compile Inventory Data – Inventory data is gathered into an electronic packet of information suitable for transmission.
c. Compile Asset Data – Intercept weapon data is gathered into an electronic packet of information suitable for transmission.
d. Transmit Data – Electronic packet of engagement evaluation data, inventory data, and asset data is transmitted to the other ships within the battle group.
e. Verify Transmission – The transmitting ship verifies that the information packet was received by the other ships within the battle group.

XXI) **End Threat Engagement –** End of successful threat engagement.

A-2 MODEL PARAMETERS: The following table is an excerpt from the EXCEL® spreadsheet that defines the parameters used to develop the Arena® simulation model. The table describes the setup for each process, and the statistical distribution used for random time based events.

TOP LEVEL	1ST LEVEL DOWN	2ND LEVEL DOWN	PARAMETERS					
			TYPE	VALUE	UNITS	ENTITIES per ARRIVAL	MAX. ARRIV	First Creation
Incoming Threat	----------	----------	Random	10	Sec	2	Infinite	0.0
			MIN. TIME	MOST LIKELY	MAX. TIME	DELAY TYPE	UNITS	ALLOCATION
Threat Detected	ID Threat	ID the Threat_Process	0.1	0.15	0.25	Triang.	sec	V.A.
	Select Preferred Sensor	Select a Preferred Sensor_Process	0.25	0.3	0.5	Triang.	sec	V.A.
	Establish Track	Establish a Track_Process	0.25	0.5	1	Triang.	sec	V.A.
	Verify Threat and Intel	Verify the Threat and Intel_Process	2	3	10	Triang.	sec	V.A.
	Update Network	Update the Network_Process	2	3	5	Triang.	sec	V.A.
	Determine Engagment Solution	Determine an Engagement Solution_Process	1	2	3	Triang.	sec	V.A.
			TYPE	Percent True				
Detecting Ship Determines FCS?	----------	----------	2-way by Chance	90%				
			MIN. TIME	MOST LIKELY	MAX. TIME	DELAY TYPE	UNITS	ALLOCATION
Relay Threat Info	Compile Data 1	Compile Data 1a	0.05	0.1	0.15	Triang.	sec	V.A.
	Transmit Data 1	Transmit Data 1a	0.05	0.3	0.4	Triang.	sec	V.A.
	Verify Transmission 1	Verify Transmission 1a	0.02	0.1	0.2	Triang.	sec	V.A.

Table B-1, Arena Simulation Model Parameters

			MIN. TIME	MOST LIKELY	MAX. TIME	DELAY TYPE	UNITS	ALLOCATION
Determine FCS	Request G1 Data	Request G1 Data_Process	0.05	0.08	0.12	Triang.	sec	V.A.
	Gather G1 Data	Gather G1 Data_Process	0.05	0.08	0.12	Triang.	sec	V.A.
	Apply Engagement Doctrine	Apply Engagement Doctrine_Process	0.1	0.15	0.2	Triang.	sec	V.A.
	Formulate Solution	Formulate Solution_Process	0.1	0.15	0.2	Triang.	sec	V.A.

			TYPE	Percent True
Will FCS Ship Coordinate Assets?	----------	----------	2-way by Chance	90%

			MIN. TIME	MOST LIKELY	MAX. TIME	DELAY TYPE	UNITS	ALLOCATION
Relay FCS Info	Compile Data 2	Compile Data 2a	0.05	0.1	0.15	Triang.	sec	V.A.
	Transmit Data 2	Transmit Data 2a	0.05	0.3	0.4	Triang.	sec	V.A.
	Verify Transmission 2	Verify Transmission 2a	0.02	0.1	0.2	Triang.	sec	V.A.

			MIN. TIME	MOST LIKELY	MAX. TIME	DELAY TYPE	UNITS	ALLOCATION
Coordinate Assets	Gather G1 Data_2	Gather G1 Data_2_Process	0.05	0.08	0.12	Triang.	sec	V.A.
	Select Weapon Type	Select Weapon Type_Process	0.05	0.08	0.12	Triang.	sec	V.A.
	Select Ship for Sensor Track	Select Ship for Sensor Track_Process	0.1	0.15	0.2	Triang.	sec	V.A.
	Select Ship for Weapon Use	Select Ship for Weapon Use_Process	0.05	0.08	0.12	Triang.	sec	V.A.
	Relay Info to Supporting Ship	Relay Info to Supporting Ship_Process	0.5	1	0.2	Triang.	sec	V.A.

			MIN. TIME	MOST LIKELY	MAX. TIME	DELAY TYPE	UNITS	ALLOCATION
Schedule Sensor and or Weapon	Contact Threat Tracking Ship	Contact Threat Tracking Ship_Process	0.5	1	2	Triang.	sec	V.A.
	Contact Firing Ship	Contact Firing Ship_Process	0.5	1	2	Triang.	sec	V.A.
	Prepare Weapon	Prepare Weapon_Process	0.5	1	2	Triang.	sec	V.A.

			TYPE	Percent True
Will Scheduling Ship Fire Weapon?	----------	----------	2-way by Chance	90%

			MIN. TIME	MOST LIKELY	MAX. TIME	DELAY TYPE	UNITS	ALLOCATION
Relay Firing Command Info	Compile Data 3	Compile Data 3a	0.05	0.1	0.15	Triang.	sec	V.A.
	Transmit Data 3	Transmit Data 3a	0.05	0.3	0.4	Triang.	sec	V.A.
	Verify Transmission 3	Verify Transmission 3a	0.02	0.1	0.2	Triang.	sec	V.A.

			MIN. TIME	MOST LIKELY	MAX. TIME	DELAY TYPE	UNITS	ALLOCATION
Fire Weapon	Provide Shipboard Power to Weapon	Provide Shipboard Power to Weapon_Process	0.5	1	1.4	Triang.	sec	V.A.
	Provide Initialization Data to Weapon	Provide Initialization Data to Weapon_Process	0.4	0.5	0.7	Triang.	sec	V.A.
	Activate Weapon Batteries	Activate Weapon Batteries_Process	1.5	2	3	Triang.	sec	V.A.
	Provide INTENT TO LAUNCH Command	Provide INTENT TO LAUNCH Command_Process	0.05	0.1	0.12	Triang.	sec	V.A.
	Assign Launch Status	[Success = 1, Failure = 2]	0.05	0.1	0.12	Triang.	sec	V.A.
	Provide Weapon Status	Provide Weapon Status_Process	0.15	0.08	0.1	Triang.	sec	V.A.

			MIN. TIME	MOST LIKELY	MAX. TIME	DELAY TYPE	UNITS	ALLOCATION
Manage Inventory	Update Inventory of Firing Ship	Update Inventory of Firing Ship Process_Process	0.1	0.2	0.35	Triang.	sec	V.A.
	Compile Data	Compile Data Process_Process	0.06	0.1	0.15	Triang.	sec	V.A.
	Transmit Data	Transmit Data Process_Process	0.05	0.3	0.4	Triang.	sec	V.A.
	Verify Transmission	Verify Transmission_Process	0.02	0.1	0.2	Triang.	sec	V.A.

			MIN. TIME	MOST LIKELY	MAX. TIME	DELAY TYPE	UNITS	ALLOCATION
Relay Inventory Info	Compile Data 4	Compile Data 4a	0.05	0.1	0.15	Triang.	sec	V.A.
	Transmit Data 4	Transmit Data 4a	0.05	0.3	0.4	Triang.	sec	V.A.
	Verify Transmission 4	Verify Transmission 4a	0.02	0.1	0.2	Triang.	sec	V.A.

Table B-1. Arena Simulation Model Parameters (Continued)

			MIN. TIME	MOST LIKELY	MAX. TIME	DELAY TYPE	UNITS	ALLOCATION
Support Engagement	Uplink Midcourse Guidance	Uplink Midcourse Guidance_Process	0.5	0.75	1.5	Triang.	sec	V.A.
	Direct Schedule Sensor for Terminal Support	Direct Schedule Sensor for Terminal Support_Process	0.5	0.75	1.5	Triang.	sec	V.A.

			TYPE	Percent True
Will Engaging Ship Evaluate the Engagement	----------	----------	2-way by Chance	85%

			MIN. TIME	MOST LIKELY	MAX. TIME	DELAY TYPE	UNITS	ALLOCATION
Relay Engagement Data	Compile Data 5	Compile Data 5a	0.05	0.1	0.15	Triang.	sec	V.A.
	Transmit Data 5	Transmit Data 5a	0.05	0.3	0.4	Triang.	sec	V.A.
	Verify Transmission 5	Verify Transmission 5a	0.02	0.1	0.2	Triang.	sec	V.A.

			MIN. TIME	MOST LIKELY	MAX. TIME	DELAY TYPE	UNITS	ALLOCATION
Evaluate Engagement	Validate Sensor Track Data	Validate Sensor Track Data_Process	0.5	1	2	Triang.	sec	V.A.
	Perform Kill Assessment	Perform Kill Assessment_Process	0.7	1	1.2	Triang.	sec	V.A.
	Mark as Miss of Kill	Mark as Miss of Kill_Process	0.05	0.1	0.12	Triang.	sec	V.A.

			TYPE	Percent True
Threat Kill?	----------	----------	2-way by Chance	90%

Table B-1, Arena Simulation Model Parameters (Continued)

			MIN. TIME	MOST LIKELY	MAX. TIME	DELAY TYPE	UNITS	ALLOCATION
Monitor and Report All Data	Compile Engagement Evaluation Data	Compile Engagement Evaluation Data_Process	0.25	0.5	1	Triang.	sec	V.A.
	Compile Inventory Data	Compile Inventory Data_Process	0.25	0.5	1	Triang.	sec	V.A.
	Compile Asset Data	Compile Asset Data_Process	0.25	0.5	1	Triang.	sec	V.A.
	Transmit All Data	Transmit All Data_Process	5	6	7	Triang.	sec	V.A.
	Verify Transmission_2	Verify Transmission_2_Process	0.7	1	1.2	Triang.	sec	V.A.

			Record?
End Threat Engagement	----------	----------	Yes

Table B-1, Arena Simulation Model Parameters (Continued)

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. ASSUMPTIONS

The following assumptions were generated based on the top-level architecture of our group's Arena simulation.

1. All ships within the Battle Group will utilize the same algorithm (decentralized decision making).
2. Back-up solution algorithm is included in each step (scheduling, firing, etc.)
1. Processing power is not a limiting factor (Dual Core/Quad Core CPUs).
2. Data fusion techniques used is independent of network data processing.
3. The system is always functioning and in a ready state prior to engagement.
4. Communication systems functioning and in a ready state prior to engagement.
5. Combat systems will function as designed with no lapses in performance.
6. Illumination is part of the Use/Scheduling sequence.
7. There are no bandwidth limitations.
8. Specific engagement objectives/thresholds have not been established.
9. Threats are detected by ship radar, not from any other source.
10. 90% of all threat detections are by the originating ship.
11. 90% of all threat engagements are handled by the originating ship.
12. The shortest time period to transmit data over the network at any data rate is greater than the longest system processing time for any ship system/component.
13. No jamming in the surrounding environment.
14. At least one ship within the Battle Group is capable of engaging the threat.
15. The network is secure.
16. All ships possess the necessary hardware and software to communicate with one another.
17. Each ship possesses the necessary minimum requirements to support track threats, compute FCS, manage inventory data, engage threats, and process engagement data.
18. Operational context groups will be based on incoming threat location with regards to battle group ship positions.

THIS PAGE IS INTENTIONALLY BLANK

APPENDIX D. GLOSSARY

OACE	The OACE is a set of loosely coupled software components based on open standards, interfaces, and services. The fundamental requirement for OACE is to provide a distributed real-time computing environment for Naval Combat Systems and Naval Weapons Systems elements. (From FORCEnet Technical Guide)
Battle Force	A standing operational naval task force organization of carriers, surface combatants, and submarines assigned to numbered fleets. A battle force is subdivided into battle groups.
Combat Identification (CID)	CID is the process of attaining an accurate characterization of detected objects in the joint battle space to the extent that high confidence, timely application of military options and weapons resources can occur. Depending on the situation, this characterization may be limited to 'friend', 'enemy', or 'neutral'. In other situations, other characterizations may be required – including, but not limited to, class, type, nationality, and mission configuration. (From JFCOM)
Command and Control (C2)	The exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission. C2 functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (From Wikipedia)

Common Operational Picture (COP)	The COP is the integrated capability to receive, correlate, and display a common tactical picture (CTP), overlays/projections (i.e., Meteorologic and Oceanographic {METOC}, battleplans, force position projections). Overlays and projections may include location of friendly, hostile, and neutral units, assets, and reference points. The COP may include information relevant to the tactical and strategic level of command. This includes, but is not limited to, any geographically oriented planning data from JOPES, readiness data from SORTS, intelligence (including imagery overlays), reconnaissance data from the Global Reconnaissance Information System (GRIS), weather from METOC, predictions of NBC fallout, and ATO data. (From CJCSI 3151.01)
Common Tactical Picture (CTP)	The CTP is derived from the Common Tactical Dataset and other sources and refers to the current depiction of the battle space for a single operation within a CINC's AOR including current, anticipated or projected, and planned disposition of hostile, neutral, and friendly forces as they pertain to US and multinational operations ranging from peacetime through crisis and war. The CTP includes location, RT and non-real time sensor information, and amplifying information such as METOC, SORTS, and JOPES. The CTP receives its information from the component's Component Consolidated Pictures (CCPs), the COP, national sources, and other producers of information that report directly to the JTF. (From CJCSI 3151.01)
Distributed Resource Management (DRM)	DRM is critical to organize efficiently the cooperation between operating systems. DRM manage all resources in a large distributed system to fulfill IFC scenario requirements and to use the resources effectively and efficiently.

Family of Systems (FoS)	A set or arrangement of independent systems that can be arranged or interconnected in various ways to provide different capabilities. The mix of systems can be tailored to provide desired capabilities dependent on the situation. (From CJCSI 3170.01B)
Functional Flow Block Diagram (FFBD)	An FFBD is a pictorial representation of some process or model of a complex system. An FFBD shows major functions, sequence of occurrence, and functional decomposition. (From Wikipedia)
FORCEnet	An operational construct and architectural framework that integrates the SEAPOWER21 concepts of Sea Strike, Sea Shield and Sea Basing by connecting warriors; sensors, networks; command and control; platforms and weapons; providing accelerated speed and accuracy of decision; and integrating knowledge to dominate the battlespace. FORCEnet provides the following capabilities: Expeditionary, multi-tiered, sensor and weapon grids; distributed, collaborative, command and control; dynamic, multi-path survivable networks; adaptive/automated decision aids; and human-centric integration.
Global Command and Control System – Maritime (GCCS-M)	GCCS-M [AN/USQ-119E(V)], previously the Joint Maritime Command Information System (JMCIS), is the Navy's primary fielded Command and Control System. GCCS-M receives, processes, displays, and manages data on the readiness of neutral, friendly, and hostile forces in order to execute the full range of Navy missions (e.g., strategic deterrence, sea control, power projection, etc.) in near-real-time via external communication channels, local area networks (LANs) and direct interfaces with other systems. (From Wikipedia)

Global Information Grid (GIG)	GIG is defined as the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems (NSS) as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DoD, National Security, and related Intelligence Community (IC) missions and functions (strategic, operational, tactical, and business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems. (From Wikipedia)
Information Exchange Requirements (IERs)	Information Exchange Requirements are statements that define a specific category of information that needs to be communicated between two parties or organizations. Most commonly IERs are used to define information exchange needs between data processing systems at two or more C2 nodes. Often IER statements are expanded to include additional parameters such as the bandwidth size, how frequently the information is exchanged, and the media over which it will be transmitted. The expanded versions of the IERs are used in modeling and simulation activities to determine or confirm the media bandwidth needed under various scenarios. (From DODCCRP)
Integrated Fire Control (IFC)	An Electronic System that locates and tracks a target, computes the data, and employs weapon to destroy it. (From Infoplease)

Interoperability	The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases. (From Joint Publication 1-02)
Joint Land Attack Cruise Missile Defense Elevated Netted Sensor System (JLENS)	JLENS is a critical enabler of the Joint Theater Air and Missile Defense (JTAMD) system of systems. It employs advanced sensors and networking technologies to provide wide-area surveillance and precision-tracking capabilities for long-duration missions with a specific focus on land-attack cruise missile defense. The JLENS enables the precision tracking and illumination radar to support surface-based air defense assets in intercepting low-altitude airborne targets at long ranges. The JLENS, with its long on-station time, complements fixed-wing sensor assets of the other services and serves as a key member of the joint theater air and missile defense architecture, which capitalizes on the synergy delivered by the integration of systems within a system. (From Air Defense)
Mission Capability Package (MCP)	A **mission capability package** begins with a network-centric operational concept, a concept of how a particular mission could be accomplished if everyone on the team were "on the net." Next an approach to command and control, organization, and doctrine that is designed for this "networked environment" is needed. Following this, the network-centric environment must be created. To complete the package, the education and training required to make it all function smoothly need to be specified. Taken together the **mission capability package** contains everything necessary to implement a network-centric concept. This approach enables a network-centric warfighting force. (From *Report on Network Centric Warfare Sense)*

Network Centric Warfare (NCW)	NCW is a new military doctrine or theory of war that seeks to translate an information advantage into a competitive warfighting advantage through robust networking of well informed geographically dispersed forces allowing new forms of organizational behavior. (From Wikipedia)
Observe, Orient, Decide and Act (OODA)	Col John Boyd developed the concept of the OODA Loop. The OODA cycle is crucial to understand if one is regularly in harms way. To effectively defeat opponents, the OODA cycle must be followed sequentially. This model can be used to dissect compressed timeframes in a logical and sequential manner.
Open Architecture (OA)	**Open architecture** is a type of computer architecture that allows users to upgrade their hardware in all of the computer hardware & components. Open architecture allows potential users to see inside all or parts of the architecture without any proprietary constraints. Typically, an open architecture publishes all or parts of its architecture that the developer or integrator wants to share. The open business processes involved with an open architecture may require some license agreements between entities sharing the architecture information (From Wikipedia)

Open System	A system that implements sufficient open standards for interfaces, services, and supporting formats to enable properly engineered modules to be utilized across a wide range of systems with minimal changes, to interoperate with other modules on local and remote systems, and to interact with users in a style that facilitates portability. An open system is characterized by the following: 1) Well defined, widely used, preferably non-proprietary interfaces/protocols; 2) Use of standards which are developed/adopted by recognized standards bodies or the commercial market place; 3) Definition of all aspects of system interfaces to facilitate new or additional systems capabilities for a wide range of applications; 4) Explicit provision for expansion or upgrading through the incorporation of additional or higher performance elements with minimal impact on the system. (From CRD)
Single Integrated Air Picture (SIAP)	The SIAP (the air track portion of the CTP) consists of common, continual, and unambiguous tracks of airborne objects of interest in the surveillance area. SIAP is derived from real-time and near-real-time data and consists of correlated air object tracks and associated information. The SIAP uses fused near-real-time and real-time data, scaleable and filterable, to support situation awareness, battle management, and target engagements. (From JFCOM)
Situational Awareness (SA)	SA is the ability to identify, process, and comprehend the critical elements of information about what is happening to the team with regards to the mission. (From U.S. Coast Guard)
System Architecture	A representation of an engineered system, and the process and discipline for effectively implementing the design for such as system. A system may consist of information, hardware and software.

Track	A set of detections, contacts, hits or observations, generated by the same real object in the environment. It is identified by a track number, and has intrinsic and derived attributes associated with it.

APPENDIX E. STATEMENT OF WORK

Title: Open Architecture as an Enabler for FORCEnet

Scope:

The tasking provided by this statement of work (SOW) supports a series of ongoing FORCEnet (Fn) studies being performed by Naval Postgraduate School MSSE (DL) students[1]. This task is unique in that it investigates tie role of Fn and the Open Architecture (OA) Functional Domain Model whereas the other tasks investigate the concept of coalition Fn and its related performance and acquisition issues.

This task is also unique in that it consists of two parts, one to be performed by the students (and is driven by the period of performance available to the students) and a second that can be performed concurrently as faculty research or as a future student project.

As noted in the Background section, there are two operationally oriented scenarios selected to validate the Fn Architecture (time-critical targeting and cruise missile defense). This study will focus on elements of the cruise missile defense problem

Background:

If FORCEnet is to be the architectural framework for naval warfare in the information age, it must deliver performance, information assurance, and quality of-service guarantees unprecedented in a system with the nodal diversity evidenced in the joint force. This challenge is best met incrementally so that existing capability is not degraded nor information security ever compromised. The design and implementation of complex systems for purposes of warfighting require a dedicated core of warfighters and system engineers trained in the art of operations analysis. Together, warfighters and engineers

[1] Two previous MSSE (DL) classes evaluated the role of FORCEnet in coalition warfare and currently there are two follow-on coalition Fn projects that are examining performance and acquisition issues.

make decisions about when and how to introduce new capabilities as technologies and operational concepts evolve in independent but integrated spirals.[2]

The FORCEnet information architecture should be thought of as a boundary between layers of functionality that is held invariant (over long periods of time), thus allowing developments to proceed independently on all sides of the boundary. In the committee's view, architecting FORCEnet is the process of defining thin waists, or boundaries, that are invariant and, when coupled with selected industrial standards and throttled with a network control system, would enable FORCEnet to evolve with advances in technology. The boundaries standardize the interfaces between the functions common to all warfare systems so as to facilitate interoperability and information sharing. Examples of boundaries that should be established include those between sensor/intelligence networks, command-and-control networks, fire-control networks, displays, and databases, as shown in Figure 5.1.

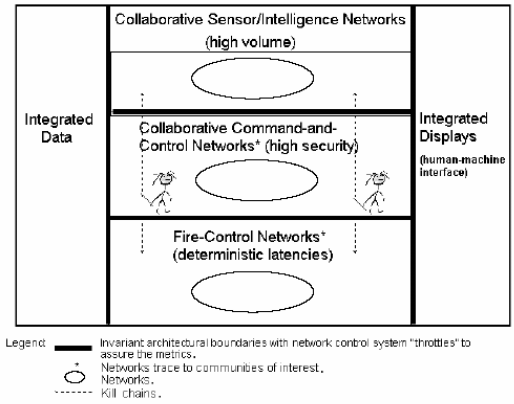

FIGURE 5.1 Examples of boundaries between functions in the FORCEnet information architecture.

The open architecture initiative (OA) addresses software reuse as well as refresh. As a result, the granularity of partitions to that utilized in legacy architectures increases and raises concerns—the number of boundaries to be maintained may exceed the number that can be reasonably managed, and the functional partitions may not be optimally placed. In particular, the committee believes that as long as functional partitioning supports the

[2] The material in this paper is extracted from Chapter 5 of FORCEnet Implementation Strategy (http://www.nap.edu/catalog/11456.html)

higher-level aggregation of interoperable functions, as suggested in Figure 5.1, it is acceptable, but the number of unique partition definitions should be minimized. The OA functional architecture shown in Figure 5.2, coupled with the FORCEnet information architecture described above, will, when implemented, greatly simplify the implementation of FORCEnet.

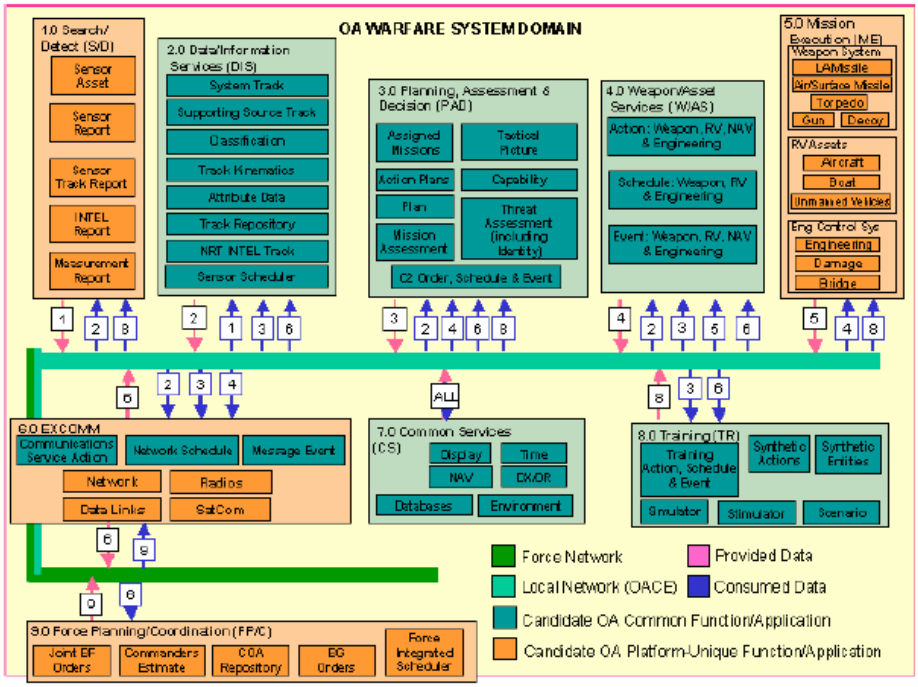

FIGURE 5.2 Open architecture functional architecture. NOTES: INTEL, intelligence; C2, command and control; NRT, near real time; RV, remotely controlled vehicle; NAV, navigation; EXCOMM, Executive Committee; SatCom, satellite communications; DX/DR, direct exchange/dead reckoning; BF, battle force; COA, common operating area; BG, battle group; OA, open architecture.

FORCEnet and the fighting units and command-and-control structure that it supports are all subsystems of a joint battle force. Systems engineering is a process for allocating functionality to subsystems that are bounded by system architecture so that the probability of mission success is optimized within available resources. A battle force performs three major functions: it manages battle, dominates battlespace, and sustains control over the battlespace over time. FORCEnet functionality is a subset of battle force functionality that can contribute to battle management, battlespace dominance, and sustainability. FORCEnet cost and contribution to battle management, battlespace dominance, and sustainability should provide a basis for implementation decisions. As a subsystem, FORCEnet must interface seamlessly with the remainder of the force while

increasing the probability of mission success more than alternative investments. Understanding and defining the interfaces between what is in the FORCEnet subsystem and what is outside of it will be an ongoing process. This top-down view of FORCEnet, together with the bottom-up work that is being done at the information architecture boundaries, is necessary to explain and quantify the warfighting value.

The FORCEnet functional architecture is based on MCPs. These are not the MCPs that the Warfare Integration Unit under the DCNO for Warfare Requirements and Programs (N70) uses for program assessment. Instead, two operationally oriented scenarios have been defined to validate the FORCEnet architecture: (1) time-critical targeting employing persistent sensors and (2) cruise missile defense.

Selected Issues

The following issues are an extract from Chapter 5 of FORCEnet Implementation Strategy (http://www.nap.edu/catalog/11456.html). This selected list captures some of the underlying research goals of this project:

1. The process and tools for translating FORCEnet operational concepts into products, services, and warfighting capabilities have yet to be fully developed. Systems engineering is a process for allocating functionality to subsystems that are bounded by system architecture.

2. The number of unique interfaces that must be maintained need to be carefully selected and kept to an absolute minimum, or evolution will be hindered by expensive and lengthy integration and testing. One way to do this is to require that systems must partition common functions in a common way.

3. There has been little attempt to characterize how FORCEnet will function in terms of network management, data flow, traffic control, nodal performance, or data access. This information is required to engineer the FORCEnet network management system.

4. The FORCEnet network controls do not provide the capability to meter and to prioritize data flow across boundaries, and FORCEnet behavior models are not developed to project performance and to support sensitivity analysis.

5. The reaction time of the joint force to sensor input is not a design-driving requirement for FORCEnet or an evaluation factor for the prioritization of activities.

Technical Requirements:

The focus of this engineering and analysis effort is to explore and develop a conceptual model that marries the operational and system Fn architecture requirements with the technical requirements of the OA Functional Domain Model. This Work will be based upon the use of three Integrated Fire Control scenarios fro references 6 and 7 to elaborate upon the basic mission capability requirements of cruise missile defense. Fn requires capabilities that enhance and enable tactical decision-making and distributed resource management. The concept for optimizing the management of distributed warfare resources is based on the premise that edge devices consisting of common data fusion processes and decision-making aids can compute common decision results or resource allocations given a foundation of shared information and knowledge. This is also the basis for the top level OA Functional Domain Model.

Statement of Work:

1. **Characterization of the problem space**: the identification of current system and legacy deficiencies as well as constraints inherent in the operational environment in order to characterize, understand and bound the problem space. The project team will translate relevant operational imperatives into system engineering structures (concepts, functions, requirements, solutions) necessary to develop the concept.

2. **Design principles**: the formulation of principles for the design and architecting of OA and Fn (IFC) capabilities. The design principles will serve as guidelines for the development of system solutions. Design principles will consider known limitations and constraints of the operational environment such as communication challenges (unreliability, ad hoc mobile networks, limited bandwidth, etc.) and operator interaction (command authority, manual overrides, etc.).

3. **Conceptual design**: the development of a vision, architecture, and conceptual framework that addresses the problem space and is based on the design principles for a distributed system of automated decision aids for optimally managing warfare resources for collaborative operations.

4. **Functional representation and decomposition**: the representation of system concepts through functional description and decomposition as well as system architecting and simulation. Develop representations, models, and methods to express automated resource collaboration concepts and solutions in the context of the Fn/OA architecture and domains.

5. **Analysis of key capabilities**: the identification and evaluation of technologies and research areas that is key to the Fn/OA concept. Technology areas that will be researched and analyzed include:
    a. Data fusion techniques and algorithms
    b. Resource management scheduling and optimization methods
    c. Weapon and sensor management for aerospace warfare
    d. Automated management aids
    e. Engagement functionality, initialization, and control
    f. Situation prediction and war-gaming
    g. Tactical planning and battle management

6. **Documentation:** The results of task 1-5 will be documented in accordance with the NPS MSSE(DL) Project Guide Requirements as modified by agreement with the project advisor.

THIS PAGE LEFT INTENTIONALLY BLANK

LIST OF REFERENCES

Clark, Vern, Admiral, United States Navy, "Sea Power 21" unveiled 17 June 2002.

Bass, Len, Paul Clements and Rick Kazman, Software Architecture in Practice, Second Edition, Carnegie Mellon, 2003

Blanchard, Benjamin, S., Walter J. Fabrycky, Systems Engineering and Analysis, Third Edition, Prentice Hall, 1998, Pages 62–71.

Buede, Dennis M., The Engineering Design of Systems, John Wiley and Sons, 2000, Pages 42–51 and 60–73.

FORCEnet Implementation Strategy, National Research Council, Council Proceedings 2005, National Academy of Sciences, Pages 115–140.

Johnson, Bonnie Worth, John M. Green, "Gaining Naval Battle Space Through Automation," 2001, National Fire Control Conference.

Johnson, Bonnie Worth, John M.Green, "Naval Network-Centric Sensor Resource Management," April 2002, Figure 6, Page 10.

Hatley, Derek, Peter Hruschka and Imtiaz Pirbhai, Process for System Architecture and Requirements Engineering, Dorset House, 2000, Pages 135–141.

Llinas, James et al., Revisiting the JDL Data Fusion Model II, (http://www.infofusion.buffalo.edu/reports/LLINAS/papers/NSSDF%20Paper%20H4%20Llinas.pdf)

Luessen, Lawrence, H., "A Self-Consistent Context for Unit- and Force-Level Tactical Decision-Making," Naval Engineers Journal, Winter 2003, Pages 67–77.

National Resource Council, FORCEnet Implementation Strategy, (http://fermat.nap.edu/catalog/11456.htmll), 2006.

Naval Forces' Capability for Theater Missile Defense, (http://fermat.nap.edu/catalog/10105.html), (2001)

Naval Integrated Fire Control-Counter Air From The Sea Draft Test and Integration Master Plan, Program Executive Office Integrated Warfare Systems (7D) (PEO IWS 7D), 14 April 2006, Page 1.

Network-Centric Naval Forces, Overview: A Transition Strategy for Enhancing Operational Capabilities, (http://fermat.nap.edu/catalog/9817.html), 2000.

Perry, Walter, Robert W. Button, Jerome Bracken, Thomas Sullivan, Jonathan Mitchell Measures of Effectiveness for the Information-Age Navy: The Effects of Network-Centric Operations on Combat Outcomes, (http://www.rand.org/pubs/monograph_reports/MR1449).

Pressman, Roger S., Software Engineering: A practioner's approach, First Edition, McGraw-Hill, 1982

———, Software Engineering: A practioner's approach, Sixth Edition, McGraw-Hill, 2005

Rushton, Captain Richard T., Mr. Michael McCrave, Mark N. Klett, Timothy J. Sorber, "Open Architecture, The Critical Network Centric Warfare Enabler, First Edition, 18 March 2004.

Shafer, Kenneth, E., Russell A. Phillippi, Simon Moskowitz, Stefan R. Allen, "Distributed Weapons Coordination Conceptual Framework," Johns Hopkins Applied Physics Laboratory, Volume 23, Numbers 2 and 3 (2002), Pages 223–235.

Schekkerman, Japp, "Adopting & Developing an Effective Enterprise Architecture for Network Centric Capability," Institute for Enterprise Architecture Developments, Part 1 Workshop, 25 August 2005, Pages 13, 17.

Steinberg, Alan N., Christopher L. Bowman, Franklin E. White, "Revisions to the JDL Data Fusion Model," 1999.

———, "The Architecture of Network Centric Warfare," Institute for Enterprise Architecture Developments, September 2005.

Strei, Captain Thomas J., "Network-Centric Applications," Open Architecture in Naval Combat System Computing of the 21st Century, 01 April 03, Figure 16, Pages 34–37.

Young, Bonnie, W., Single Integrated Air Picture Operational Concept, 2002 Command and Control Research Technology Symposium, Page 10.

———, "A C2 System for Future Aerospace Warfare," 2004 Command and Control Research Technology Symposium, Figures 7, 8, 9, 10, Pages 21–26.

———, Integrated Fire Control for Future Aerospace Warfare, Bonnie Young, Northrup Grumman Mission Systems, Pages 1–21, August 2004.

———, Combat Identification for Naval Systems in an Open Architecture, 16 January 2006, Written for Program Executive Office Integrated Warfare Systems (PEO IWS), Page 1–16

THIS PAGE LEFT INTENTIONALLY BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California